Санкт-Петербургский государственный университет

направление «Юриспруденция»

**Международно-правовое регулирование сотрудничества в борьбе с преступлениями, совершенными с использованием компьютерных технологий**

Выпускная квалификационная работа

студента 2 курса магистратуры

очной формы обучения

Лапшиной Дарья Васильевны

Научный руководитель:

доктор юридических наук, доцент Марусин Игорь Станиславович

Санкт-Петербург

2017 год

**Содержание**

[Введение 3](#_Toc481956330)

[Глава 1. Понятие преступления, совершаемого с использованием компьютерных технологий 7](#_Toc481956331)

[Глава 2. Общее и специальное регулирование киберпреступлений в международном праве 21](#_Toc481956332)

[2.1 Регулирование киберпреступлений нормами общего международного права 21](#_Toc481956333)

[2.2 Специальное регулирование, связанное непосредственно с преступлениями, совершаемыми с использованием компьютерных технологий. 40](#_Toc481956334)

[Конвенция Совета Европы о киберпреступлениях (2001) 40](#_Toc481956335)

[Европейский Союз 50](#_Toc481956336)

[СНГ 53](#_Toc481956337)

[3. Проблемы реализации международно-правового сотрудничества в сфере борьбы с преступлениями, совершенными с использованием компьютерных технологий 56](#_Toc481956338)

[3.1 Разграничение юрисдикции государств в отношении киберпреступлений 56](#_Toc481956339)

[3.2 Национальное право государств, применимое к определению киберпреступлений. 63](#_Toc481956340)

[Заключение 71](#_Toc481956341)

# Введение

Преступление, совершаемое с использованием компьютерных технологий как значимое международное явление, впервые было упомянуто в «The Criminal Justice Resource Manual on Computer Crime», подготовленном для Департамента Юстиции США в 1979 г.[[1]](#footnote-1) Данный вопрос был поднят в связи с активизацией внутригосударственных преступлений, совершаемых посредством сетей: в 1973 г. кассир нью-йоркского Ситибанка, перевел на свой счет 2 млн. долларов, использовав служебный компьютер, в 1988 г. было рассмотрено первое дело о незаконности доступа хакера к компьютеру третьего лица,[[2]](#footnote-2) а уже в 1989 г. американским студентом было заблокировано около 6000 ЭВМ Пентагона. За два года до выхода вышеуказанного руководства, после демонстрации возможностей международного действия сети ARPANET, Правительство США отмечало, что сети подобного типа не могут быть использованы для противозаконных целей и выражало обеспокоенность по поводу увеличения объема преступлений, совершаемых посредством информационных сетей и компьютеров.

Фактически, началом эры преступлений, совершаемых с использованием компьютерных технологий являлось появление первой группы хакеров, студентов Массачусетского Института Технологий, которые и изобрели термин «hacking». Их деятельность не была направлена на совершение противоправных действий: они не создавали угроз ни для сетей, ни для компьютеров. Лишь десять лет спустя, формулировка «хакеры» приобрела негативную характеристику: хакеры стали угрозой общества, не только ввиду совершения уголовных преступлений, но и ввиду политических акций в США, что связывалось с деятельностью негативно настроенных Юппи. Несмотря на широкое использование сети Интернет в дальнейшем, киберпреступления стали также угрозой для частных, локальных сетей.

Несмотря на расцвет киберпреступлений еще в конце 1980-ых, международное правовое поле в данной сфере стало значительно расширяться только в 90-ых годах XX века. Национальное право к тому моменту имело значительное развитие, связанное в первую очередь с преступлениями экономического характера, будь то мошенничество или незаконный доступ к данным. Международное право отреагировало на такие преступления в первую очередь как на угрозу миру и безопасности, связанному с возможностями вероятных материальных последствий, что теоретически можно расценивать как преступление агрессии.

Тем не менее, на практике расследования киберпреступлений долгое время было достаточно нерациональным: следственные органы, не обладавшие должным арсеналом инструментов для расследования преступлений, совершенных с использованием компьютерных технологий не могли осуществлять должного преследования хакеров за их преступления. Также на раскрытие преступлений, совершенных с использованием компьютерных технологий влияло законодательство, которое в некоторых случаях просто не имело такого состава преступлений.

Главной гипотезой настоящего исследования является предположение о недостаточности международно-правового регулирования сотрудничества в сфере преступлений, совершенных с использованием компьютерных технологий.

Актуальность данного исследования, исходя из вышеизложенного, обусловлена техническим прогрессом, усилением трансграничных угроз, связанных с компьютерными технологиями, тенденцией разработки международно-правового регулирования с долгосрочным отставанием и длительным отсутствием консенсуса между государствами в области регулирования преступлений, совершаемых с использованием компьютерных технологий.

Целью выпускной квалификационной работы являлось определение основным проблем международного сотрудничества в сфере борьбы с преступлениями, совершаемыми с использованием компьютерных технологий.

Задачами исследования являлись определение общего термина «преступление, совершенное с использованием компьютерных технологий», выделение общего международного регулирования, применимого к преступлениям, совершенным с использованием компьютерных технологий, исследование существующих международных договоров в области компьютерных преступлений, анализ существующего международного и национального регулирования преступлений, совершаемых с использованием компьютерных технологий, выделение и поиск разрешения проблем в соответствующей сфере.

Объектом исследования является международно-правовое сотрудничество в сфере борьбы с преступлениями, совершенными с использованием компьютерных технологий. Предмет исследования – международно-правовые акты и национальное законодательство в сфере борьбы с преступлениями, совершенными с использованием компьютерных технологий.

Теоретическая значимость исследования определена тем, что комплекс теоретических выводов и положений вносит определённый вклад в систему научных знаний о природе, сущности и регулировании преступлений, совершенных с использованием компьютерных технологий.

Практическая значимость заключается в возможности использования результатов и выводов исследования в работе органов государственной власти Российской Федерации, разработки предложений по совершенствованию международно-правового регулирования преступлений, совершенных с использованием компьютерных технологий и уголовного законодательства в соответствующей сфере.

Научная новизна работы обусловлена объектом исследования, который недостаточно разработан в теории международного права, комплексным характером рассмотрения институтов национального уголовного права и международного права и полученными результатами, в первую очередь прикладного характера.

В ходе проведенного исследования автору не удалось обнаружить комплексных исследований, посвященных рассматриваемой теме. Вопрос регулирования преступлений, совершенных с использованием компьютерных технологий неоднократно поднимался в исследованиях российских ученых, однако непосредственно в контексте международного права, он рассматривался Дэвидом С. Уоллом, А.Г, Волеводзом, М. Шмиттом, А.Д. Гудманном. Необходимо отметить, что большинство исследований проводились до 2010 года, что определяет необходимость актуализации исследований в настоящей сфере.

# Глава 1. Понятие преступления, совершаемого с использованием компьютерных технологий

Преступления, совершаемые с использованием компьютерных технологий – относительно недавнее явление в праве.

Основной особенностью таких преступлений является использование специфичных инструментов, способов, включающих в себя не только компьютеры или компьютерные программы, а также уникальное сочетание способа и объекта преступления, в котором объектом и инструментом одновременно может быть информационная сеть или компьютерная программа. Международный Союз Электросвязи, занимающийся в первую очередь техническим определением действий, которые могут попадать понятие преступлений, совершаемых с использованием компьютерных технологий, определяет несколько характерных для них черт:[[3]](#footnote-3)

- преимущественно международный характер преступлений;[[4]](#footnote-4)

- компьютеры являются и средством совершения преступления, и, зачастую, целью;

- совершение преступлений в рамках информационных сетей.

В настоящее время отсутствует консенсус в вопросе единой дефиниции таких преступлений. Большинство источников, даже при интенсивном оперировании термином «преступление, совершенные с использованием компьютерных технологий», не раскрывает понятия такого преступления. В связи с быстрой эволюцией информационных технологий, как таковых, компьютерные технологии стали меняться настолько быстро, что формирование всеобъемлющего термина стало затруднительным.

ООН использует термин «*киберпреступление*» как собирательное нейтральное понятие[[5]](#footnote-5), выведенное из существующих в национальных системах.[[6]](#footnote-6) Национальное право оперирует различными терминами: киберпреступления,[[7]](#footnote-7) компьютерные преступления[[8]](#footnote-8), преступления, совершаемые с использованием информационных технологий[[9]](#footnote-9), преступления в сфере высоких технологий[[10]](#footnote-10), и т.д. В связи с этим, в дальнейшем автор работы использует формулировку «киберпреступление» как тождественную понятию «преступление, совершаемое с использованием компьютерных технологий».

На настоящий момент, международное право не содержит универсального понятия киберпреступления, закрепленного в международном договоре. Существовали несколько попыток создания такого термина на уровне Организации Объединенных Наций и региональных организаций.

На 10 Конгрессе ООН по предупреждению преступности и обращению с правонарушителями 2000 г. были рассмотрены две категории киберпреступлений и обозначены два определения киберпреступлений. Первая дефиниция, более широкая, определяет киберпреступление как преступление, связанное с использованием компьютеров (“computer-related crime”) и, соответственно, как «любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети».[[11]](#footnote-11) Вторая дефиниция, определяющая киберпреступление в узком смысле, приравнивает его с компьютерным преступлением (“computer crime”), то есть любым противоправным деянием, осуществляемым посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных.

Эксперты уточняют, что первая дефиниция («computer-related crime») фактически представляет собой круг правонарушений,[[12]](#footnote-12) поскольку криминализация таких деяний сильно разнится в разных государствах, и преступлений (к которым также относятся описанные во второй категории). Невозможно изолировать те составы, которые относятся к категории преступлений в определенных государствах, но относятся к категории правонарушений в иных.

Эта «плавающая» категория представляет собой границу уголовной ответственности в национальном праве. Различия в законодательствах государств, касающиеся уголовной либо иной ответственности, также будут иметь эффект для правоприменительной практики, при которой разрешение спора о праве, ввиду неясности места совершения преступления, будет иметь негативный эффект, поскольку, учитывая в большинстве случаев трансграничный эффект киберпреступлений, наличие в национальном законодательстве какого-либо состава преступления и отсутствие в другом будет препятствовать привлечению к ответственности преступника.[[13]](#footnote-13) Так, Управление ООН по наркотикам и преступности отмечает, что применение термина «киберпреступление» в большинстве случае зависит от конкретного случая.[[14]](#footnote-14)

Также отмечается, что широкое толкование данного преступления включает в себя практически все незаконные действия, связанные с компьютером (computer-related crimes) включая в себя распространение вирусов, взлом аккаунтов и иные действия, которые не могу быть классифицированы как преступления. Но в узком смысле киберпреступления включают в себя наиболее тяжкие правонарушения и преступления, для совершения которых используются компьютерные и иные информационные технологии (в частности Интернет).

Организация Североатлантического договора (НАТО) разработала Таллиннское Руководство – рекомендательный документ, разработанный специалистами в области международного права по инициативе Центра НАТО по киберобороне, - не оперирует понятием киберпреступления или подобным термином, однако, поскольку, что сферой исследования было применение права в кибервойне, оно оперирует достаточно точными правовыми понятиями, описывающими явления в сфере компьютерных технологий. В связи с этим, следует учитывать правовую основу в этой области, выработанную Таллиннским Руководством.

Однако, единого понимания и унифицированной дефиниции киберпреступления на настоящий момент в международном праве нет. Это связано с различными подходами в объекте посягательства, различными субъектами преступлений и роли компьютерных технологий в совершении таких преступлений.

В связи с длительным развитием киберпреступности, следует рассмотреть несколько подходов, применяемых для рассмотрения объектов посягательства преступлений, связанных с компьютерными технологиями.

Во-первых, различают преступления, направленные против компьютерной системы и киберинфраструктуры.

*Аппаратное обеспечение* или же hardware представляет собой «физические компоненты, которые включают в себя компьютерную систему и киберинфраструктуру».[[15]](#footnote-15) *Компьютерная система*[[16]](#footnote-16) – это один или несколько соединенных устройств с соответствующим программным обеспечением и периферическими устройствами, которые осуществляют автоматизированную обработку данных.

Так, аппаратное обеспечение включает в себя «мозг» и «тело»: киберинфраструктура представляет собой ресурсы, поддерживающие коммуникацию, хранение и вычисления компьютерных данных, позволяющие компьютерной системе функционировать.

*Компьютерные данные*, то есть информация, обрабатываемая или создаваемая компьютерной системой при автоматизированной обработке данных, являются основным объектом большинства преступлений, совершаемых с использованием компьютерных технологий. Они не имеют материального или физического воплощения, и являются частью киберпространства, о чем подробно будет рассказано позже.

Если преступления против компьютерной системы и данных, совершаемые в киберпространстве, в большинстве случаев выделены специальными нормами, и фигурируют в национальном законодательстве, то нападение на киберинфраструктуру не настолько однозначно, хотя последствия таких преступлений могут быть достаточно серьезными.[[17]](#footnote-17)

Преступления, объектами посягательства которых является киберинфраструктура, возможно совершить, как в киберпространстве, так и в материальном мире. Выведение из строя киберинфраструктуры, например, сервера, возможно путем кибератаки (DDos – атаки) или путем физического уничтожения. Оба метода приведут к выведению киберинфраструктуры из строя, либо нарушает ее функционирование, но одно будет совершено через киберпространство, а другое – в реальном мире.

Проблема в различии объектов, которая представляется недостаточно явной, может иметь достаточные последствия для квалификации преступлений. Она заключалась в нечетком описании компьютерной системы как средства или объекта совершения преступления. Так, под описание второго термина попадали также преступления, в которых элементы ввода или вывода информации являлись физическим средством совершения преступления: убийства, грабеж или разбой т.д.

Нападения, совершаемые в реальном мире в большинстве государств обеспечены соответствующим регулированием, в то время как нападение на киберинфраструктуру в киберпространстве не регламентированы.

Данный аспект ведет к различиям в квалификации атак на компьютерные системы, как основной объект киберпреступлений. Формально, инфраструктура представляет часть компьютерной системы, но последствия атаки на нее могут быть различными. Может быть совершено преступление, в котором главным объектом будет объект критической инфраструктуры, обеспечиваемый определенным комплексом аппаратного обеспечения.

В связи с этим возникают несколько вопросов. Насколько компьютерные системы зависят от киберинфраструктуры или ее части и возможно ли действие таковой без нее? В каждом отдельном случае эффект от выведения из строя киберинфраструктуры следует оценивать отдельно. Также, следует оценивать последствие атак на киберинфраструктуру критической инфраструктуры: медицинские системы, связанные с диагностикой, системы анализа уровня воды гидроэлектростанций. Тем не менее, атаки на киберинфраструктуру рассматриваются как часть нападения на компьютерную систему, учитывая характер и их взаимодействие.

Во-вторых, киберпреступления могут быть направлены на компьютерные системы или информационные сети.

Киберпреступления могут совершаться не только при воздействии на изолированный компьютер, но и при использовании информационных сетей, то есть дистанционно. Настоящее различение в квалификации связано с развитием сети Интернет. Этот критерий влияет на определение места преступления, и, соответственно, юрисдикции и, в некоторых случаях – применимого права.

Происходит различие компьютера как обособленного комплекса устройств и компьютерных технологий, объединенных общим управлением и информационной сети, наиболее обширной из которых является Интернет.

Одним из примеров разделения таких категорий преступлений является Конвенция Совета Европы о киберпреступлениях 2001 года. Настоящая Конвенция определяет компьютерную систему как устройство или группу устройств, если хотя бы одно из них осуществляет автоматизированную обработку данных. На момент создания Конвенции, подразумевалось, что данный термин будет охватывать исключительно компьютерные устройства, как персональные настольные компьютеры. Основным критерием выделения компьютерных систем является автоматизированная обработка данных, то есть осуществление процесса компьютерной программы, как комплекса инструкций, исполняемых компьютером для достижения результата, вне какого-либо прямого воздействия на нее человека. В таком смысле компьютерная система – это компьютер (процессор, осуществляющий автоматизированную обработку данных)[[18]](#footnote-18), к которому могут быть присоединены периферические устройства ввода или вывода.

Однако, в пояснении к ст. 1 Конвенции, указывается, что компьютерные системы могут быть соединены сетью между двумя или более системами вне зависимости от способа такого соединения. Такие сети могут быть как локальными, так и глобальными (Интернет), поскольку главной чертой такого соединения является возможность передавать данные. В travaux preparatories настоящей конвенции, компьютерные преступления, какими они стали дальше в соответствии с формулировкой Конвенции, описывались как «преступления, совершенные в киберпространстве». Отдельно выделялись преступления, для совершения которого использовались коммуникационные сети, в связи с чем выделялись отдельные виды преступлений, таких как незаконные денежные операции, нарушение авторских прав и иные.

Конвенция Совета Европы применяет термин «киберпространство», представляющее собой общее пространство, создаваемое пользователями информационных сетей путем коммуникации между собой и информационными сервисами.[[19]](#footnote-19)

Международный Союз Электросвязи[[20]](#footnote-20), «Таллинское руководство по международному праву, применимому в кибервойне», Международная организация стандартизации[[21]](#footnote-21) и дают схожие определения киберпространства, как среды, сформированной физическими и не физическими компонентами и характеризуемой использованием компьютеров и электромагнитного спектра для сохранения, модификации или обмена информацией при использовании компьютерных сетей.

Киберпространство является новой «площадкой» совершения преступлений. Вопросы о фактических способах реализации там каких-либо действий следует адресовать специалистам по информационным технологиям непосредственно. С правовой точки зрения является неопределенным момент о применении к этому пространству существующих норм права: может ли право, применяемое к одной «реальности» быть применимым к киберпространству.

В киберпространстве невозможно определить границы государств, и, соответственно, границы реализации суверенитета и применения законодательства. Особую сложность представляет тот факт, что киберпреступление из материального мира переходит в совершенно иную плоскость, преследование в которой доставляет не только материальные, но и процессуальные проблемы при расследовании таких деяний. Понятие киберпространства является удобным для применения в практике ввиду своей умышленной размытости, так оно будет наиболее длительное время сохранять свою актуальность. Киберпространство, как элемент понятия «киберпреступление» является наиболее важным: преступления, совершаемые в киберпространстве, подлежат отличному регулированию, нежели преступления, совершаемые в материальном мире. Поскольку некоторые киберпреступления могут повторять составы уже имеющихся преступлений, их регулирование может быть идентичным, но последствия применения права непосредственно и применение такого права зависит в первую очередь от места совершения преступления, каковым можно считать киберпространство.

Рассматривая вышеизложенное, следует отметить, что в каждой национальной системе обычно присутствуют составы преступлений, связанные с компьютерными системами, но игнорируются вопросы киберинфраструктуры, приравнивая нападения на них к нападению на компьютерные системы. Также отсутствует четкое разделение преступлений, совершаемых с использованием информационных сетей и отдельных компьютерных систем.

Третьим различием, препятствовавшим эффективному сотрудничеству и унификации понимания концепции киберпреступления, являлось различие в квалификации таких преступлений в части субъектов преступлений. Предполагается, что на настоящий момент этот вопрос является пережитком прошлого, тем не менее, значительно повлиявшим на развитие законодательства о киберпреступлениях.

Изначально термин «киберпреступление» рассматривался как совершенно новая категория преступлений, совершаемых «белыми воротничками».[[22]](#footnote-22) Отличительной особенностью киберпреступлений называли в первую очередь активную интеллектуальную работу: в отличие от каких-либо преступлений, требующих физического воздействия или хотя бы физического присутствия, киберпреступления совершались с применением инструмента, не отражавшего никаких данных о преступнике абсолютно, но требовавших определенного уровня знаний и грамотности. В связи с этим, первое определение киберпреступления, рассмотренное в международном аспекте было следующим: «совершение любого противоправного деяния, для которого знание компьютерных технологий является существенным для совершения преступления».[[23]](#footnote-23)

Но вскоре возникла проблема киберпреступлений как деяний лиц, в большинстве своем обладающими специальными знаниями без какой-либо профессиональной подготовки. Одним из наиболее громких дел, связанных с таким аспектом, является дело Петерсена.[[24]](#footnote-24) Оно являлось одним из первых, рассматривавших вопрос о непрофессиональных киберпреступниках. Гражданин США Петерсен был осужден за несколько эпизодов компьютерной кражи, незаконного доступа к компьютерам федерального назначения, краж с банковских карт, перехвата электронных коммуникаций и иных действий. Им была подана апелляция, основанная, среди прочих, на аргументе об отсутствии специальной подготовки к работе с компьютером в целом. На момент принятия решения, в законодательстве США существовала норма, согласно которой действия преступника оценивались строже, если имело место злоупотребление публичным или частным доверием, а также наличие специальных навыков, облегчавших совершение таких преступлений. То есть пользователи, обладавшие специальными навыками, представлялись обществу наиболее опасными. Апелляционный Суд на такой аргумент ответил толкованием нормы и пришел к выводу, что для наличия «специальных навыков» не требуется обучение, практика или лицензия работы с компьютерами. В дальнейшем данная норма была исключена из законодательства США. Так, признано, что преступления, совершаемые с использованием компьютерных технологий, представляют собой преступление с общим субъектом, а не специальным, в связи с чем совершаются повсеместно, с каждым годом расширяя круг преступников.

Несмотря на почти унифицированное понимание преступлений, совершенных с использованием компьютерных технологий, с их разделением на различные категории и применением национальных норм, возникают несколько практических проблем. Преступления, совершаемые через информационные сети, в виду обширности таковых, могут совершаться как в государстве нахождения устройства, так и в ином государстве, в то время как преступления, совершаемые с использованием только изолированного устройства, имеют местом своего совершения территорию того государства, на территории которого и находятся этот компьютер. Вопрос юрисдикции также отмечался в Конвенции Совета Европы, предполагая, что именно этот аспект является наиболее спорным для государств.[[25]](#footnote-25) Различные виды юрисдикций представляют собой международную проблему не только в части преступлений, совершаемых с использованием компьютерных технологий, [[26]](#footnote-26) но и с иными преступлениями.

Вышеуказанные различия позволяют сделать вывод о том, что киберпреступления разделяются на несколько видов, хотя и отражают единое явление – преступление, совершенное с использованием в том или ином виде компьютерных технологий. Тем не менее, для целей международного сотрудничества вопрос универсального определения представляется существенным.

Ввиду отсутствия универсального определения, закрепленного на международном уровне, следует обратиться к практике государств в области киберпреступлений.

Право Соединенных Штатов Америки выделяет наибольший, на настоящий момент, список киберпреступлений, однако также не дает определения киберпреступления. Кодекс законов США выделяет преступления, совершаемые с использованием компьютерных преступлений в следующих категориях: незаконный доступ к устройству,[[27]](#footnote-27) мошенничество и ложные сведения, мошенничество с использованием почты и иные преступления, связанные с мошенничеством[[28]](#footnote-28), злоумышленное повреждение имущества, непристойное поведение, кража собственности, сексуальная эксплуатация и иное жестокое обращение с детьми, перемещение в целях сексуальной эксплуатации и соответствующие преступления.[[29]](#footnote-29) Также существует отдельный раздел, посвященный азартным онлайн-играм.[[30]](#footnote-30)

Киберпреступления в законодательстве Великобритании регулируются отдельным актом – Законом о нецелевом использовании компьютеров 1990 г.,[[31]](#footnote-31) составляющим Закон о серьезных преступлениях. Как и Кодекс США, он не содержит определения киберпреступлений, однако перечисляет виды преступлений, попадающих под действие Акта: несанкционированный доступ к компьютерным материалам,[[32]](#footnote-32) несанкционированный доступ с намерением совершить или облегчить совершение новых преступлений,[[33]](#footnote-33) несанкционированные действия с намерением нанести ущерб или с безразличием в отношении работы компьютера и т.д.,[[34]](#footnote-34) несанкционированные действия, вызывающие или создающие риск серьезного ущерба.[[35]](#footnote-35) Последний состав преступления внесен в 2015 году, и, фактически, вносит поправки, касающиеся серьезного ущерба благополучию людей либо национальной безопасности. Такой шаг обусловлен активизацией мощных кибератак, имеющих последствия в материальном мире.

Закон о кибербезопасности Китая 2016 г. наоборот, не содержит конкретного списка преступлений, однако описывает в целом обязанности государства по предотвращению киберпреступлений. Отдельно рассматривается вопрос критической информационной инфраструктуры, касающейся публичных услуг, водоснабжения, финансов, управления и некоторые иные.[[36]](#footnote-36) Однако, термин «критическая информационная инфраструктура» в Законе не раскрывается. Достаточная часть обязанностей возлагается на провайдеров сетей. Например, вводится система мониторинга и хранения данных в сетях о деятельности пользователей,[[37]](#footnote-37)

Большинство государств содержат комплексное определение киберпреступления как преступления, связанного с Интернетом или компьютерными системами,[[38]](#footnote-38) некоторые же выделяют отдельно преступления, в которых компьютерная система является целью и способом совершения преступления.[[39]](#footnote-39) Такой же позиции придерживаются исследователи, выделяя отдельно киберпреступление как преступление, связанное с Интернетом и компьютерными технологиями. [[40]](#footnote-40)

Обращаясь к доктринальным источникам, следует отметить высокий уровень смешения различных терминов, относимых к киберпреступлениям.[[41]](#footnote-41) Так, Black’s Law Dictionary определяет «киберправо» («cyber»), как регулирование, связанное с Интернетом.[[42]](#footnote-42) Оксфордский словарь определяет киберпреступление как совершаемое с использованием Интернета или любой другой сети. [[43]](#footnote-43)

Выведение всеобъемлющего правового термина затруднительно по ряду причин. [[44]](#footnote-44) Во-первых, наличие технического элемента в определении не позволяет рассматривать преступления подобного рода как цельную юридическую конструкцию, для определения состава которой возможно избежать участия экспертов в области компьютерных технологий в каждом конкретном случае. Во-вторых, компьютерные технологии представляют собой постоянно изменяемую и развивающуюся структуру, описание которой будет регулярно изменяться, что, в свою очередь, препятствует эффективному правоприменению. В-третьих, большинство преступлений имеют транснациональный характер, в котором преступник и его жертва находятся в разных государствах, и минимальное различие в формулировках представляет собой лазейку, позволяющую неосуществление правосудия в одном государстве, что будет нарушать права потерпевшего. Но, обращаясь ко второй причине, универсальное определение, в силу его моментального старения, будет различаться для наиболее развитых и развивающихся государств, автоматически создавая пробел в праве.

Киберпреступления можно разделить на несколько видов, которые отдельно выделяет национальное законодательство множества государств, однако, для создания международного договора следует изначально договориться о терминах, которые значительно разнятся в различных государствах, что затрудняет международное сотрудничество.

Обобщая вышеизложенное, следует сделать вывод о том, что понятие «киберпреступление» представляет собой незаконное деяние, совершаемое в киберпространстве и направленно против компьютерных систем, компьютерных данных, либо совершенное с использованием компьютерной системы.

Данное определение является наиболее общим. Тем не менее, существуют значительные различия в общем понимании термина «преступления, совершенные с использованием компьютерных технологий», обусловленных различным пониманием связи этих преступлений с компьютерными технологиями. Это не позволяет создать единый объект обсуждения, что исключает эффективное сотрудничество государств в данной сфере.

# Глава 2. Общее и специальное регулирование киберпреступлений в международном праве

Как было указано ранее, несмотря на активное развитие концепции киберпреступлений в национальном законодательстве, в международном праве отсутствуют универсальные международные договоры. В связи с этим, следует рассмотреть существующее правовое регулирование в области международного права, которое потенциально может регулировать сферу киберпреступлений и специальное регулирование, касающееся исключительно таких преступлений.

## 2.1 Регулирование киберпреступлений нормами общего международного права

Все преступления, преследуемые по международному праву или затрагивающие его, можно подразделить на международные преступления и преступления международного характера (или конвенционные преступления).

К международным преступлениям[[45]](#footnote-45) относят наиболее серьезные преступления против мира и безопасности человечества, наказуемые по международному праву.[[46]](#footnote-46) К ним относят преступление агрессии,[[47]](#footnote-47) геноцид,[[48]](#footnote-48) преступления против человечности,[[49]](#footnote-49) преступления против персонала ООН и связанного с ней персонала,[[50]](#footnote-50) и военные преступления.[[51]](#footnote-51)

Преступления международного характера в свою очередь влекут наказание по национальному праву, в то время как составы таких преступлений, в силу их серьезности и общественной опасности, содержатся в международных договорах. Международные договоры (в большинстве своем конвенции, в связи с чем, в некоторой литературе употребляется термин «конвенционные преступления»)[[52]](#footnote-52) содержат нормы, обязующие предотвращать и наказывать лиц, виновных в совершении рассматриваемых в конвенции преступлений; реализовать такие обязательства возможно при имплементации в национальное законодательство соответствующих положений.[[53]](#footnote-53)

К преступлениям международного характера относятся международный терроризм, пиратство, преступления, связанные с оборотом наркотиков и множество иных, мнения о признании которых таковыми различаются в большинстве государств.

***Международные преступления***

Преступление агрессии, в соответствующей Резолюцией Генеральной Ассамблеи[[54]](#footnote-54) и, содержащей идентичные нормы, ст. 8-bis Римского Статута,[[55]](#footnote-55) определяется как подготовка, инициирование или осуществление акта агрессии лицом, имеющим возможность осуществлять руководство или контроль за политическими либо военными действиями государства. Акт агрессии в свою очередь представляет собой применение вооруженной силы государством или группой государств против другого государства вне зависимости от его признания или участия в ООН, являющимся серьезным масштабным нарушением норм, содержащихся в Уставе ООН. Перечень действий,[[56]](#footnote-56) квалифицируемых как агрессия, не является закрытым, но правом определения агрессии в каждом конкретном случае наделе исключительно Совет Безопасности ООН.[[57]](#footnote-57)

Для данного преступления основным является дефиниция «применения вооруженной силы» (use of force), так или иначе фигурирующая в определении.

Запрет применения вооруженной силы является обычной нормой права[[58]](#footnote-58) и допускает исключения в случае самообороны,[[59]](#footnote-59) контрмер[[60]](#footnote-60) или действий Совета Безопасности в соответствии со ст. 42 Устава ООН. Однако, ввиду специфики рассматриваемого субъекта, возникают вопросы, касающиеся его применимости к вышеуказанному термину.

Действия, совершаемые с использованием компьютерных технологий, могут представлять собой такие преступления. Термин «кибератака» стал особо популярным после массовой компьютерной атаки на Эстонию.[[61]](#footnote-61) Однако, вопрос о том, стоит ли считать ситуацию в Эстонии ситуацией применения вооруженной силы, остается открытым, поскольку доказательств действия киберпреступников как подконтрольных государству представлено не было.

Международный Суд ООН в деле «Никарагуа против США» сделал вывод о том, что тренировка и финансирование США контрас хоть и были вмешательством во внутренние дела Никарагуа, но представляли собой применение вооруженной силы.[[62]](#footnote-62) Обращаясь к данному положению, следует сделать вывод о том, что под применением силы подразумевается действие, приводящее исключительно к физическому ущербу.[[63]](#footnote-63)

В ситуации в Эстонии не было физического ущерба, человеческих жертв или каких-либо материальных последствий. Но существовал серьезный ущерб компьютерным системам, что не может оставаться без внимания. В связи с чем часть исследователей полагает, что преступление агрессии может быть совершено в киберпространстве, если оно схоже по масштабу и эффекту с операциями, проводимыми вне киберпространства.[[64]](#footnote-64)

Это является первым вопросом о том, в какой степени серьезными должны быть последствия атаки в киберпространстве и как можно соотнести последствия в материальном мире и в киберпространстве. Если условием такого преступления является наличие материального ущерба или человеческих потерь, может ли атака на какой-либо управляющий сервер, которая не привела к его физическому уничтожению, быть признана применение вооруженной силы, даже если последствием станет невозможность дистанционного воздействия на объекты критической инфраструктуры, нарушение связи, необходимой для поддержания обороны государства? Такие действия не имеют материальных последствий, и в соответствии с вышеуказанным выводом Международного Суда, не могут расцениваться как применение силы. На взгляд автора, подобные действия имеют серьезные последствия и могут быть квалифицированы как преступление агрессии, даже если их последствия отражаются только в киберпространстве.

Другим вопросом является вопрос об осуществлении контроля над непосредственными исполнителями. Лицо, совершающее преступление агрессии должно фактически осуществлять контроль или руководство за действиями государства. Данный критерий позволяет отграничивать преступление агрессии как действие от лица государства[[65]](#footnote-65) от иных преступлений. В отличие от эффективного контроля, реализуемого в обычном вооруженном конфликте, в котором государство непосредственно участвует в разработке конкретных планов и инструкций,[[66]](#footnote-66) при совершении аналогичного преступления в киберпространстве становится практически невозможно определить лицо, которое должно быть ответственно за данное преступление.

Также, поднимая вопрос о возможности ответственности государства за такие преступления, в частности, при рассмотрении вопроса о частных группах исполнителей, также существуют сложности в присвоении действий лиц государству. Ярким примером является непринятие государством мер по противодействию совершению преступления,[[67]](#footnote-67) расцениваемое как принятие государством действий частных лиц как собственных.[[68]](#footnote-68) В связи с этим следует обратить внимание на практический вопрос: в большинстве случаев государства не могут выявить преступников, совершающие национальные преступления, будет ли возможность расследования случая международного преступления? Также, учитывая возможность практически полной анонимизации в киберпространстве, данные, характеризующие последний оставленный «след» в сети, в частности IP-адрес, могут не отражать объективной действительности: в связи с возможной цепью переадресации потоков информации от изначальной точки до конечной через множество провайдеров и серверов, указанный IP-адрес может являться последним отслеженным, но не изначальной точкой атаки.

Несмотря на кажущуюся предопределённость и невозможность совершения военного преступления путем использования компьютерных технологий, следует отметить, что несмотря на отсутствие прецедентов, существует практическая возможность реализации подобных действий, расцениваемых как военные преступления.

Римский Статут Международного Уголовного Суда, отразивший обычную норму международного права о военных преступлениях, определяет таковые как серьезные нарушения Женевских конвенций от 12 августа 1949 года, либо иные серьёзные нарушения законов и обычаев войны как во время международного или немеждународного вооруженного конфликта, совершаемых в рамках плана либо при широкомасштабном совершении таких действий при осознании наличие вооруженного конфликта.[[69]](#footnote-69)

Действия, так или иначе запрещенные международным гуманитарным правом, подпадающие под действие jus in bello и составляют основу военных преступлений. Преступления, совершаемые с использованием компьютерных технологий, также могут попадать под определение таковых несмотря на способ совершения таких действий.

В то же время, представляется сложным проведение актов геноцида посредством киберпреступлений, поскольку осознание наличия принадлежности лица к конкретной охраняемой группе и намеренное истребление такой группы представляется достаточно сложным. Тем не менее, это возможно при применении определенных способов, чаще медицинских, то есть имеющих конкретное, выборочное действие на определенного человека. В частности, при использовании компьютерных систем наблюдения за телом человека, которые имеют непосредственное влияние на его здоровье (сердечные стимуляторы и иные),[[70]](#footnote-70) однако практическое воплощение выборочных действий представляется достаточно сложным.

***Конвенционные преступления***

Некоторые исследователи полагают, что киберпреступления представляют собой prima facie преступление международного характера. На взгляд автора работы, данная точка зрения не может быть серьезно воспринята ввиду отсутствия ***универсальной*** договорной нормы, признающей преступления с использованием компьютерных технологий незаконными. Вероятно, характеристика киберпреступления как преступления международного характера связана с транснациональностью[[71]](#footnote-71) данных преступлений.

Киберпреступления, как было указано ранее, могут быть и непосредственно самостоятельными преступлениями, а могут быть лишь способом совершения иных преступлений. Таким образом, следует выделить две группы: киберпреступления как транснациональные конвенционные преступления и непосредственно конвенционные преступления, совершаемые с помощью компьютерных технологий.

**Киберпреступления как транснациональные преступления**

То, что киберпреступления имеют транснациональный характер, было отмечено Интерполом еще в 1979 г.[[72]](#footnote-72) В отличие от перечисленных преступлений международного характера, в настоящий раздел включаются отдельные составы преступлений, взаимодействующих непосредственно с компьютерными технологиями. Такие виды преступлений могут являться одновременно самостоятельным преступлением и способствовать совершению иных преступлений.

Преступления в киберпространстве попадают под критерии, выделенные в Конвенции ООН против транснациональной организованной преступности 2000 г.:

1. Преступление, признанное таковым в данной Конвенции

или

1. Серьезное преступление, носящее транснациональный характер[[73]](#footnote-73) и совершенное при участии организованной преступной группы

Конвенция 2000 г. указывает в качестве преступлений несколько составов. Однако, в виду специфики исследования, рассмотрению подлежат только некоторые из них.

Совершение серьезного преступления, связанного с получением материальной выгоды при наличии сговора и наличие действия хотя бы одного участника признается преступлением по Конвенции, если это предусмотрено внутренним законодательством.

Наличие сговора имеет место в большинстве случаев киберпреступлений.[[74]](#footnote-74) Несомненно, существуют "индивидуалисты", однако группы хакеров действуют более эффективно как в совершении преступлений, в которых объектом является компьютер, так и при совершении иных преступлений, в которых применяются компьютерные технологии. Сложность в определении наличия преступной группы может стать технический вопрос: некоторые виды атак используют автоматизированные системы или управляемые компьютерные системы, в связи с чем количество хакеров на первый взгляд искусственно увеличивается, несмотря на фактическую компактность такой группы.[[75]](#footnote-75)

Коллектив киберпреступников может быть организован традиционно, в структурно оформленной группе, либо в форме организованной группировки. Первый вид применяется в группе, созданной для совершения одного преступления. Такие группы преимущественно занимаются экономическими преступлениями.[[76]](#footnote-76) Организованные группы в большинстве случаев имеют политический и/или идеологический характер. Организованные группы встречаются значительно реже, в зачастую состав таких групп быстро изменяем, и целью таких групп является взлом систем, либо иные атаки на компьютерные системы, либо пиратством.[[77]](#footnote-77) Однако, ввиду совершения преступлений в киберпространстве, сложно выяснить не только количество участников группы, но и форму ее создания. [[78]](#footnote-78)

Одним из примеров наиболее известных случаев сложностей в квалификации является группировка Anonymous,[[79]](#footnote-79) которая, предположительно, не имеет иерархической структуры, лидера, а также постоянного состава участников. Любой пользователь Интернета может способствовать деятельности группировки, устанавливая специальное программное обеспечение, позволяющее задействовать ресурсы компьютерной системы для совершения DDos – атак в качестве компьютера – «зомби», что затрудняет идентификацию лиц, участвовавших в атаке, и способ организации такой группы. Тем не менее, скоординированное нападение на один объект может свидетельствовать о минимальном сговоре преступников.

Киберпространство представляет множество возможностей для совершения таких преступлений, имеющих особую специфику. Одной из таких возможностей является использование виртуальных валют.[[80]](#footnote-80) Поскольку, использование Интернета позволяет использовать удаленные услуги, преступники разбивают суммы незаконно полученных денег и отправляют их в различные банки различных государств. Несколько таких переводов, зачастую, приводят к конфликтам юрисдикций государств и не позволяют эффективно расследовать подобные преступления. Усложняются такие схемы переводом реальных денег в виртуальные – Bitcoin[[81]](#footnote-81) и использованием возможностей онлайн игр.

Единственным решением привлечения преступников, чьи действия связаны с киберсферой, к ответственности являются прогрессивные методы расследования киберпреступлений. Однако, неэффективность и несвоевременность[[82]](#footnote-82) множества мер, предпринимаемых правоохранительными органами, отмечалась как препятствие международному сотрудничеству.

Ко второй группе, выделенной Конвенцией, относятся «серьезные преступления», совершаемые с целью получения материальной выгоды и при участии организованной преступной группы. К киберпреступлениям общего плана, попадающим под определение транснациональной преступности, следует отнести незаконный доступ, незаконный перехват, незаконное вмешательство, мошенничество, и иные. Однако, формулировка «серьезное преступление» как преступление, наказываемое лишением свободы не менее 4 лет, либо более строгой мерой наказания, представляется неэффективной.[[83]](#footnote-83) Применяемый в Конвенции критерий зависим от национального законодательства и, поэтому, достаточно неточен для целей назначения наказания за киберпреступления. В то же время, Конвенция предполагается включение составов киберпреступлений в сферу действия: предполагается, что транснациональные преступления могут совершаться с использованием компьютерных технологий.[[84]](#footnote-84) В подготовительных документах фигурировала идея о включении некоторых киберпреступлений в сферу действия Конвенции,[[85]](#footnote-85) но она не нашла отражения в конечном варианте Конвенции.

В связи с этим возникает вопрос о целесообразности применения норм Конвенции к киберпреступлениям, поскольку в настоящем случае гармонизация норм представляется несущественной в связи со значительными различиями в национальном законодательстве.[[86]](#footnote-86) Следует предположить, что введение в национальное законодательство «устоявшихся» в практике киберпреступлений, указанных в Конвенции Совета Европы о киберпреступлениях, а также установление одного наказания за такие преступления будет способствовать развитию межгосударственного сотрудничества. Однако, вероятно это невозможно ввиду национальных различий в использовании компьютерных систем и киберпространства (в частности, Китая). Хотя следует отметить, что при создании Конвенции, была выдвинута точка зрения, согласно которой не следует включать в определение транснациональной преступности вид и срок наказания.[[87]](#footnote-87) Но унификация в части конкретного указания в конвенции на срок лишения свободы, в частности в контексте киберпреступлений, представляется нерациональной: различия в национальном законодательстве в части квалификации преступлений и видов наказания, учета специфики преступлений и их многообразия не позволяют государствам расценивать наказание в одинаковом ключе и применять критерий срока, указанного в Конвенции.[[88]](#footnote-88) В то же время, учитывая цели, которые преследовали создатели Конвенции и Протоколов к ней,[[89]](#footnote-89) создание соответствующего протокола о киберпреступлениях будет более эффективным, чем помещение киберпреступлений в рамки ст. 3(2).

**Кибертерроризм.**

Международному терроризму посвящено множество международных договоров как универсального,[[90]](#footnote-90) так и регионального уровней. Однако, универсального определения терроризма не существует.[[91]](#footnote-91) Определение терроризма можно косвенно вывести из Международной конвенции о финансировании терроризма. В соответствии со ст. 2, терроризмом являются деяния (кроме указанных в соответствующих договорах, прилагаемых к Конвенции), направленные на смерть или тяжкие телесные повреждения гражданского или иного лица, или лиц, не принимающего активного участия в военных действиях в ситуации вооруженного конфликта с целью запугать население либо заставить правительство или международную организацию совершить либо не совершать какое-либо действие.[[92]](#footnote-92)

Специальный трибунал по Ливану в 2011 г. выдвинул собственное определение, согласно которому терроризм представляет собой совершение преступления (будь то убийства, похищения человека, взятия в заложники и т.д.) или угроза его совершения, направленная на распространение страха среди населения, зачастую направленная на создание публичной опасности, либо прямо или косвенно принудить государство или международный орган предпринять какое-либо действие, либо воздержаться от него, когда такое преступление имеет транснациональный характер.[[93]](#footnote-93)

Терроризм является одним из «многоликих» конвенционных преступлений. Ему посвящено около 15 международных договоров ООН и бесчисленное множество региональных договоров. Однако, национальное право, несмотря на международные источники, самостоятельно привносит специфические черты при имплементации такого преступления: некоторые государства включают в определение терроризма ущерб собственности,[[94]](#footnote-94) а иные – акцентируют внимание на возможной объективной уголовной юрисдикции.[[95]](#footnote-95) В связи с этим следует отграничивать состав терроризма по национальному или международному праву.

Терроризм, совершаемый посредством компьютерных технологий, часто называют с «кибертерроризмом». Множество исследований посвящено кибертерроризму как отдельному транснациональному преступлению.[[96]](#footnote-96)

Автор настоящей работы полагает, что для целей международного права преступления, совершаемые с использованием компьютерных технологий, являются лишь способом совершения преступления, приводящего в дальнейшем к последствиям терроризма как конвенционного преступления. Однако, в связи с новыми угрозами, следует провести анализ понятия «кибертерроризма», широко используемым в последнее время.

Например, понятие «кибертерроризм», выводимое Центром стратегических и международных исследований (США, Вашингтон DC), рассматривается как «использование компьютерных сетевых инструментов для воздействия на критическую национальную инфраструктуру (энергию, транспорт, государственные операции), либо для принуждения или запугивания государства или гражданского населения.»[[97]](#footnote-97) Нападение на объекты критической инфраструктуры[[98]](#footnote-98) может значительно снизить безопасность как государства, так и населения.[[99]](#footnote-99) Представляется разумным включение состав международного терроризма положений о нападении на объекты критической инфраструктуры, поскольку такие действия провоцируют достаточно опасные последствия, которые невозможно было предвидеть десять лет назад. Примером таких нападений могут служить кибернападения в США в 2001 г.[[100]](#footnote-100) и 2003 г.,[[101]](#footnote-101) когда действия в киберпространстве имели серьезные материальные и политические последствия. В 2001 году кибернападению подверглась система обеспечения электричеством США, в 2003 и позже была серия нападений на компьютерные системы федерального правительства США.

Следует отметить, что современные реалии предоставляют иные возможности для нападения на объекты критической инфраструктуры. Например, возможное действие ЭМИ (электро-магнитного излучения),[[102]](#footnote-102) также может привести к выводу объектов из строя. В связи с этим, включение в международно-правовое регулирование отдельно нападения в киберпространстве на объекты критической инфраструктуры, нецелесообразно.

Также среди объектов нападения рассматривается inter alia, собственность частных лиц как объектов некритической инфраструктуры[[103]](#footnote-103) или киберинфраструктуры.[[104]](#footnote-104) Однако, учитывая цели международных конвенций в области терроризма, следует заметить, что нападение на данный состав не представляет такой общественной опасности и, в большинстве случаев, не может привести к тяжким последствиям. С такой точкой зрения можно поспорить, и в качестве примера привести WikiLeaks, которая пополнялась посредством раскрытия данных не только из анонимных источников. Незаконные действия против компьютерных систем[[105]](#footnote-105) также имели место быть и вопрос о том, соотносимы ли последствия раскрытия конфиденциальной информации государственного масштаба[[106]](#footnote-106) с последствиями терроризма. Также, в связи с вышеуказанным примером, следует отметить, что некоторые исследователи выделяют также в качестве объекта терроризма информацию и компьютерные программы. На взгляд автора, невозможно приравнять такие действия к действиям против государственных компьютерных систем. Тем не менее, это не отменяет незаконности таких действий.

Необходимо заметить, что терроризм, как одно из наиболее опасных преступлений, в целом преследует определенные цели: запугать население, принудить к чему-либо государство. Многие исследователи рассматривают кибертерроризм вне контекста вышеуказанной цели[[107]](#footnote-107) и рассматривают любое нападение в киберпространстве как терроризм,[[108]](#footnote-108) что, на взгляд автора, является недопустимым с правовой точки зрения.

Вопрос о том, что киберпространство позволяет воздействовать на критическую инфраструктуру, остается открытым: международно-правовое регулирование не указывает на такой объект нападения. Но в силу потенциальной опасности таких нападений,[[109]](#footnote-109) следует включить критическую инфраструктуру в число объектов терроризма. Для реализации такого регулирования, по мнению автора, будет рациональным принять отдельный международно-правовой акт, сфера действия которого будет распространяться на кибертерроризм, приводящий к материальным последствиям (как смерть или тяжкие телесные повреждения) и терроризм в целом направленный на объекты критической инфраструктуры.

В связи со спецификой киберпространства возникает множество практических вопросов. Одной из проблем является возможность присвоения действий террористов государству, что может быть расценено не как акт терроризма, а вооруженный конфликт.[[110]](#footnote-110) В связи с этим, существуют практические проблемы привлечения лиц к ответственности.

Международные организации предпринимают попытки урегулирования такого вопроса в русле непосредственно киберпреступлений, однако на настоящий момент существуют только рекомендательные акты.[[111]](#footnote-111)

Международный терроризм многолик. Он может принимать различные формы: против гражданской авиации и судоходства, ядерный и бомбовый терроризм, терроризм, связанный с захватом заложников. Также, в киберпространстве могут быть совершены различные преступления, способствующие развитию терроризма в целом: пропаганда, вербовка, публикации и иные действия.[[112]](#footnote-112) Для целей настоящего исследования, данные вопросы в контексте применения компьютерных технологий, несмотря на возможность их глубокого анализа, рассмотрены не будут.

**Преступления, связанные с наркотическими средствами**

Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 г. рассматривает в качестве преступлений международного характера производство, продажу, поставку, транспортировку, импорт или экспорт наркотических средств,[[113]](#footnote-113) культивирование определенных видов наркотиков,[[114]](#footnote-114) организацию, руководство или финансирование преступлений, указанных выше,[[115]](#footnote-115) а также перевод собственности, если она получена в результате вышеуказанных правонарушений и определенных действий, связанных с собственностью, полученной в ходе действий, рассматриваемых Конвенцией как преступлений.[[116]](#footnote-116) Более ранние Конвенции (Единая Конвенция о наркотических средствах 1961 года и Протокол к ней 1972 года о поправках к Единой конвенции о наркотических средствах 1961[[117]](#footnote-117) и Конвенция о психотропных веществах 1971 года[[118]](#footnote-118)) практически полностью покрывают весь возможный массив преступлений, связанных с наркотическими средствами.

Интернет позволяет эффективно совершать практически все вышеуказанные преступления. Анонимность, масштаб, возможность создания целых «рынков» сбыта – все это делает киберпространство площадкой массовых преступлений, связанных с наркотиками. На настоящий момент продажа наркотиков через Интернет является едва ли не наиболее распространенным преступлением. Даркнет кишит индивидуальными магазинами и даже целыми рынками, объединяющими множество покупателей и продавцов. Одной из наиболее масштабных и эффективных платформ является “Silk Way” (Шелковый Путь), копирующий известные e-Bay и Amazon. При этом все данные покупателей и продавцов зашифрованы, система Tor шифрует все данные о входящих и исходящих с платформы. При оплате применяются биткоины, что делает наркотрафик практически неуловимым.

Практически все составы преступлений описаны в Конвенции ООН, но вопрос о применимости ее составов к отношениям в киберпространстве остается открытым. С иной стороны, киберпространство не меняет самостоятельного состава преступлений, то есть совершение таковых в киберпространстве не меняет практически ничего. На взгляд автора, также не представляется логичным изменять или уточнять нормы конвенции при 189 участниках.[[119]](#footnote-119)

**Детская порнография**

Детская порнография, торговля детьми и детская проституция признаны в качестве преступлений большинством государств: участниками Факультативного протокола к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии являются 173 государства.[[120]](#footnote-120) Факультативный протокол, будучи достаточно современным, отражает, что распространение детской порнографии в Интернете является недопустимым.[[121]](#footnote-121) В таком направлении рассуждает и Комитет по правам ребенка, предлагая государствам включить в национальное законодательство положения о детской порнографии в Интернете.[[122]](#footnote-122) Тем не менее, детская порнография как оставалась, так и остается проблемой многих государств.[[123]](#footnote-123) Также, Даркнет имеет в обращении множество площадок, содержащих детскую порнографию.

Но если Факультативный Протокол был в большей степени направлен на ограждение детей от такого вида действий, то компьютерные технологии позволяют в полной мере создавать такого рода порнографию.[[124]](#footnote-124) Целью Факультативного Протокола являлось ограждение детей от такого отношения. Национальное законодательство большинства государств[[125]](#footnote-125) содержит положения о запрете детской порнографии с том или ином виде, но лишь единицы включают в законодательство вопрос о созданной детской порнографии посредством компьютерных технологий.[[126]](#footnote-126) Протокол, как было указано ранее, не покрывает цели пресечения создания «искусственной порнографии», что не создает проблем в материальном праве, но создает проблемы в общем этическом отношении к такому аспекту. Тем не менее, данный вопрос лежит вне области международного права прав человека – отсутствует объект защиты, в таком случае применять какие-либо шаги на международном уровне представляется нецелесообразным. Так, Европейским Союзом предприняты меры по гармонизации законодательства в сфере «создаваемой» детской порнографии.[[127]](#footnote-127) Подобные положения отражены в Лансаротской конвенции и Конвенции Совета Европы о киберпреступлениях.[[128]](#footnote-128)

Но Интернет опасен не только самой детской порнографией, но и склонением к ней. Так, дети подвергаются опасности домогательств,[[129]](#footnote-129) последствия которых сходны с детской проституцией, запрещенной Протоколом. Тем не менее, следует учитывать, что такой аспект имеет в большей степени национальный характер, поскольку вопрос сексуального согласия в различных государствах варьируется.

Подводя итог, следует отметить, что общее международно-правовое регулирование лишь частично затрагивает киберпреступления, норм, содержащихся в общем международном праве недостаточно для регулирования киберпреступлений. Существующие международные конвенции не включают в сферу действия большинство преступлений, составы которых характерны для киберпреступлений. Также, большинство из них не предполагают регулирования преступлений в киберпространстве. Также представляется проблемным то, что что некоторые государства не желают приравнивать преступления в киберпространстве к преступлениям, которые происходят в «реальном мире», применение вышеуказанных норм затрудняется различными подходами к такой проблеме.

Поскольку регулирование нормами общего международного права, предназначенного для регулирования преступлений, совершаемых в материальном мире, не всегда может быть применимо к преступлениям, совершенным в киберпространстве. Так, общего регулирования может быть недостаточно: большинство международных договоров не предусматривают возможности применения их положений над преступлениями в киберпространстве. Ввиду недостаточности общего регулирования следует разработать специальный международный договор в сфере киберпреступлений. Подготовка новых международных договоров об особых видах киберпреступлений, представляется достаточно релевантной и разумной, несмотря на то, что, в некоторых случаях создание новых международных актов не приветствуется ввиду обширности существующих международно-правовых инструментов.

## 2.2 Специальное регулирование, связанное непосредственно с преступлениями, совершаемыми с использованием компьютерных технологий.

К сожалению, на настоящий момент, существует малое количество международных инструментов, связанных с криминализацией киберпреступлений. Однако, существует множество рекомендательных актов, в особенности международных организаций, которые с наступлением эры Интернета не могут не затрагивать киберпространство и различные аспекты, связанные с ним.

## Конвенция Совета Европы о киберпреступлениях (2001)

Указанная Конвенция является первым и наиболее авторитетным на настоящий момент международным договором, связанным с компьютерными преступлениями. Совет Европы, несмотря на фактическую невозможность издания обязательных документов,[[130]](#footnote-130) стал инициатором создания Конвенции, участником которой на настоящий момент являются не только члены Совета Европы, но и иные государства.[[131]](#footnote-131) Предполагалось, что создание Рекомендации, не имеющей обязательного характера для участников, будет недостаточным для разрешения столь серьезной проблемы:[[132]](#footnote-132) поскольку существовало множество рекомендательных документов, создание еще одного не позволило бы наладить эффективное сотрудничество в этой области.

Конвенция Совета Европы рассматривает составы преступлений, совершаемых с использованием компьютерных технологий. Вопрос таких преступлений был вынесен на уровень международного сотрудничества, создавая основу для имплементации положений не только государств-участников такой Конвенции, но и стимулируя иные государства обратить внимание на проблему киберпреступлений. В связи с этим, в настоящем исследовании ей будет уделено особое внимание, как одному из наиболее успешному в своей реализации международному договору.

В процессе становления вопроса киберпреступлений, Совет Европы прошел долгий путь. В частности, были изданы несколько Рекомендаций Совета Министров. Первая, направленная на имплементацию норм о преследовании преступлений, связанных с компьютерами, 1989 г., впервые касалась тематики киберпреступлений.[[133]](#footnote-133) Вторая, 1995 г., затрагивала общие вопросы уголовного процесса, технического обеспечения органов следствия и электронных доказательств.[[134]](#footnote-134)

Работа над Конвенцией о компьютерных преступлениях началась в 1997 г. с момента создания Комитета Экспертов по преступлениям в киберпространстве при Европейском Комитете по проблемам преступности,[[135]](#footnote-135) что было обусловлено стремительным развитием информационных технологий в целом.[[136]](#footnote-136)

Целью Конвенции являлась унификация национального уголовного права, содержащего элементы преступлений, совершаемых и связанных с киберпреступлениями, а также создание правовых условий для осуществления достаточного расследования и преследования подобных преступлений и установление режима эффективного сотрудничества в настоящей сфере.[[137]](#footnote-137)

Конвенция содержит 4 главы: первая содержит основные понятия, используемые с Конвенции, вторая раскрывает содержит меры материального и процессуального характера, необходимые для принятия на национальном уровне Государствами-участниками, третья глава рассматривает порядок международного сотрудничества. Четвертая – заключительная часть, в частности регулирующая вступление Конвенции в силу.

Конвенция рассматривает киберпреступления как преступления, связанные с компьютером (computer-related crimes), а в дальнейшем выделяет отдельные виды, подобные тем, что приведены автором в первой главе. В Пояснительном Докладе уточнено, что список преступлений, рассматриваемых Конвенцией, представляет собой «минимальный консенсус»[[138]](#footnote-138), и не включает в себя множество иных преступлений, которые могут иметь место в национальном законодательстве. В своей сущности, список преступлений Конвенции является выборкой наиболее актуальных преступлений на 2001 год с возможностью проекции установленных норм на развивающиеся технологии.

Стоит отметить, что часть 1 («Материальное уголовное право») содержит в большей степени описание преступлений, которые должны быть криминализованы в государстве-участнике, но не представляет собой строгую норму и предусматривает наличие множества вариаций, уточняемых в Пояснительном Докладе. Это обусловлено тем, что терминологически составы преступлений могут значительно отличаться, а жестко установленные нормы, не соответствующие существующим нормам национального права, могли бы снизить привлекательность Конвенции как международного договора.

Поскольку большинство норм, указанных в подразделах 2 (правонарушения, связанные с использованием компьютерных средств), 3 (правонарушения, связанные с содержанием данных) и 4 (правонарушения, связанные с нарушением авторского права и смежных прав) так или иначе имели место в национальном законодательстве, особое внимание будет уделено нормам подраздела 1, составы преступлений, отраженные в которых, направлены против конфиденциальности, целостности и доступности компьютерных данных и систем и были восприняты большинством государств-участников как новые и подлежащие имплементации или обновлению. Особое рассмотрение представляется также необходимым, поскольку Конвенция содержит достаточно лаконичные описания, и дополняется Пояснительным Докладом.

Норма ст.2 Конвенции содержит состав **противозаконного доступа**. Им является преднамеренный и неправомерный доступ, то есть проникновение, к компьютерной системе (в целом либо в ее части), совершенный с нарушением мер безопасности и умыслом либо на завладение компьютерными данными, либо с иным умыслом в отношении какой-либо компьютерной системы. Противозаконный доступ направлен против компьютерных систем и компьютерных данных.

Данная норма фактически включает в себя два состава преступления: противозаконный доступ к компьютерным системам и противозаконный доступ к компьютерным данным. Следует заметить, что данное преступление, по замыслу авторов, не может быть совершено без подключения к телекоммуникационной сети, локальной, либо глобальной,[[139]](#footnote-139) но это не отражено в тексте Конвенции, что делает обращение к Пояснительному Докладу необходимым.

**Незаконный перехват[[140]](#footnote-140)** угрожает в первую очередь данным.

Незаконный перехват (Illegal interception) – это неправомерный перехват данных (включая электромагнитные излучения, несущие компьютерные данные), непредназначенных для общего пользования, передаваемых в компьютерную систему, либо в нее или из нее, совершаемых умышленно и с использованием технических средств. Норма может быть изменяема, поскольку государства могут включать также условия наличия умысла или компьютерной системы, соединенной с иной компьютерной системой. Если не прибегать к Пояснительному Докладу, норма представляется достаточно объемной. Следует предположить, что настоящий состав преступления указывает в большей степени на возможность нарушения киберинфраструктуры: отдельно упоминаются электромагнитные излучения, несущие компьютерные данные, которые, вероятно, рассматривались как общее понятие и для радиоволн, и для последующих технологий, использующих подобный вид связи (Wi-Fi, Bluetooth). Так, фактически можно сказать, что целью перехвата может быть телекоммуникационная сеть, но не только компьютерная система.

Технические средства в контексте настоящей нормы никаким образом не поясняются ни в Конвенции, ни в Пояснительном Договоре, который указывает что к таковым могут быть отнесены средства прослушивания, мониторинга сообщения телекоммуникационных сетей, либо компьютерные системы (или их части, например, средства ввода или вывода), либо средства перехвата и записи данных сетей.[[141]](#footnote-141) Так, к объективной стороне этого преступления будут относиться не только прослушивание и перехват в режиме реального времени, но и запись сообщения сети.

Если предыдущая статья указывает лишь возможность доступа и записи данных, то ст. 4 Конвенции рассматривает возможность **изменения** этих **данных** в любой возможной форме. Так как данные могут выступать в форме компьютерных программ, следует отметить, что основным методом совершения такого преступления является использование вируса или вредоносного программного обеспечения.[[142]](#footnote-142) Государства могут включать такой признак, как серьезный ущерб для преследования настоящих действий.

Ст. 5 рассматривает такой состав преступления, как **воздействие на функционирование системы (компьютерный саботаж)**.[[143]](#footnote-143) Состав этого преступления представляет собой деяния, указанные в ст. 4 Конвенции, направленные на умышленное создание неправомерно серьезных помех при функционировании компьютерной системы. В качестве методов воздействия при совершении этого преступления могут использоваться разнообразные виды инструментов: от DDos-атак до рассылки спама.[[144]](#footnote-144) Тем не менее, основной должна быть оценка последствий, а не способ совершения преступления.

**Злоупотребление использованием устройства** (ст. 6) представляет собой использование компьютерной системы для совершения киберпреступления: использование ее для незаконного доступа, DDos – атак, производства вирусов или потенциально опасных программ.[[145]](#footnote-145) В такой ситуации, компьютерная система представляет собой инструмент или способ совершения преступления, а не объект, как в предыдущих составах преступления. Пароли и иная информация, которая может содействовать получению доступа к компьютерным системам для дальнейшего злоупотребления использованием компьютерной системой также запрещаются к распространению или производству. Изначально создатели Конвенции полагали, что включение в сферу данного положения всех устройств будет разумным, однако в финальной версии было решено, что характер устройства сам по себе не имеет значения, в то время как оно должно быть разработано или адаптировано в первую очередь для совершения преступлений. То есть, устройства двойного назначения исключены из сферы действия данной статьи.

Далее следуют нормы подразделов 2-4, которые, как было оговорено выше, рассмотрены не будут.

Конвенция учитывает дополнительные виды ответственности, включающие покушение или иные виды соучастия,[[146]](#footnote-146) корпоративную ответственность[[147]](#footnote-147) и статью о применяемых санкциях и мерах.[[148]](#footnote-148)

Часть 2 содержит процессуальные нормы. Они и стали камнем преткновения при ратификации Конвенции. В частности, Российская Федерация отказалась ратифицировать Конвенцию по причине угрозы некоторых процессуальных вопросов ее суверенитету.[[149]](#footnote-149)

Авторы Конвенции полагали, что сбор информации и международное сотрудничество должно производиться не только в отношении преступлений, указанных в Конвенции, но и в отношении иных преступлений, совершение которых может затрагивать интересы других государств.[[150]](#footnote-150) К тому же, данная норма позволяет обеспечивать достаточный уровень сотрудничества, необходимого не только для реализации Конвенции как международного договора, но и в целом принципа сотрудничества государств. Также, предусматривается включение в национальное законодательство норм об использовании электронных (digital) доказательств в уголовном процессе,[[151]](#footnote-151) что позволяет «компьютеризировать» процесс: в частности, восприятие доказательств на информационных носителях позволяет проводить расследования преступлений с наибольшей эффективностью, поскольку перенос информации с носителя на «реальное» доказательство (например, часть вредоносного кода на бумагу) будет усложнять восприятие правоприменителями такого доказательства, когда восприятие электронного доказательства может быть облегчено средствами компьютерных технологий.

Авторы Конвенции тщательно проработали вопрос электронных доказательств и электронного сотрудничества. Государства должны предпринять меры по внесению в законодательство мер по сохранению государственными органами информации на протяжении 90 дней, особенно если существует риск ее утери или изменения.[[152]](#footnote-152) Тем не менее, государства не должны сохранять всю информацию, проходящую по трафику каналов, они должны быть убеждены, что такая информация существует.[[153]](#footnote-153) Касательно персональных данных, вопрос о сохранении которых в таком порядке в большинстве государств является абсолютно новым,[[154]](#footnote-154) которые тоже проходят по каналам связи, государства должны предпринять меры, которые включали бы исключения в вопросе персональных данных для целей уголовного преследования и судопроизводства.[[155]](#footnote-155) Для реализации такой меры, следует предпринять ряд иных, в частности – урегулировать вопрос о поставщиках услуг, которые, в свою очередь, могут не предоставлять данные о потоках информации, проходящих по его каналам. Полномочные органы, в соответствии с Конвенцией, должны иметь право на то, чтобы отдавать распоряжения о предоставлении информации лицам на территории государства или поставщику услуг, услуги которого доступны на территории этого государства.[[156]](#footnote-156)

Данный вопрос вызывал особо активную реакцию у провайдеров и международных организаций, поскольку запись такого количества информации привел бы к огромным расходам. Также раскрытие таких данных могло бы привести к злоупотреблению органов власти.

В качестве конкретных уголовно-процессуальных мер, Конвенция предлагает обыск и выемку хранимых компьютерных данных, сбор в режиме реального времени и перехват данных о содержании. Если первый метод известен большинству национальных правовых систем, то два последних, при злоупотреблении, могут представлять собой нарушение этой же самой Конвенции. Тем не менее, для совершения таких преступления недостаточно обыденных знаний о компьютерных системах и доступа к контролируемым данным. В этот момент происходит возвращение к специальным лицам, обладающим соответствующими знаниями. Момент, касающийся непосредственно регламентации таких процедур, оставлен на усмотрение национального законодателя. Однако, следует отметить, что предлагаемые Конвенцией меры не раз становились предметом рассмотрения Европейского Суда по правам человека.[[157]](#footnote-157)

Конвенция также поднимает вопрос юрисдикции государств над киберпреступлениями. В ст. 22 отмечает возможность реализации юрисдикции над преступлениями, совершенными на территории государства, борту судна или самолета, плавающего/зарегистрированного по законам этого государства, либо совершенными одним из граждан, если правонарушение является наказуемым в месте совершения преступлениям, либо это правонарушение совершено за пределами территориальной юрисдикции какого-либо Государства (открытое море, космос).[[158]](#footnote-158) Однако, создатели сознательно не включили в этот список юрисдикцию иных государств, даже если то заявило об отсутствии желания/возможности привлечь лицо к ответственности, что, даже при соблюдении правовых формальностей в части запроса на выдачу, может нарушать принцип *aut dedere aut judicare.* Например, Норвегия отказалась выдавать США российского гражданина, подозреваемого в распространении компьютерного вируса. При этом, Норвегия и США являются участниками Конвенции.

Отмечая особенности преступлений, совершаемых с использованием компьютерных технологий, Конвенция рассматривает вопрос конфликта юрисдикций.[[159]](#footnote-159) Конфликтующие Государства – Участники должны производить консультации с целью определения наиболее подходящей юрисдикции. Каким бы юридически верным не было это положение, оно заметно отягчается практической стороной вопроса реализации юрисдикции – институтом выдачи, регламентация которого в Конвенции также не влечет эффективного сотрудничества в этой области.

Наиболее любопытным нововведением следует считать процедуру передачи информации и установление системы 24/7 – контактного центра, деятельность которого направлена на оказание технической помощи и помощи в процедурных аспектах сбора и обеспечения сохранности информации, то есть, фактически, исполняющая аспекты международного сотрудничества по Конвенции.[[160]](#footnote-160) Так как Конвенция касается множества процессуальных вопросов, ее нормы заменяют или корректируют несколько актов Совета Европы.[[161]](#footnote-161) Процедуры, установленные Конвенцией, обладают эффективностью за счет доступа к передачам конкретных компьютерных данных, сохранению таких данных и возможности сохранять трафик и перехватывать данные в режиме реального времени. Однако, такие процедуры могут угрожать правам человека, либо же суверенитету государств ввиду трансграничной передачи данных. Также, Конвенция предусматривает создание конкретных процедур и систем.

Конвенция СЕ стала примером и катализатором развития для других государств и международных организаций. Например, Содружество Наций (Commonwealth of Nations) создало модельный закон о международном сотрудничестве в области преступлений, совершаемых с использованием компьютерных технологий, практически списав положения Конвенции. Также, Содружество Наций принимает самое активное участие в развитии киберправа в государствах и является наблюдателем Комитета, созданного в соответствии с Конвенцией Совета Европы о киберпреступлениях.[[162]](#footnote-162)

Также, Комитетом по Конвенции о киберпреступлениях регулярно проводится аналитическая работа[[163]](#footnote-163) и исследования по конкретным вопросам,[[164]](#footnote-164) касающимся уточнения некоторых положений, раскрытия возможности применения Конвенции к некоторым видам преступлений.[[165]](#footnote-165)

Следует отметить также статус настоящей Конвенции. Любопытным представлялся механизм вступления в силу этого международного договора: Конвенция подлежит ратификации (принятию, утверждению) пяти государств, из них как минимум три должны быть государствами-членами Совета Европы.[[166]](#footnote-166) Такой вариант вступления в силу Конвенции открыл возможности для присоединения не только государств-членов Совета Европы, но и других государств, чем таковые воспользовались. На настоящий момент, участниками Конвенции являются 53 государства – 43 государства-участника и 10 не участвующих в Совете Европы Государств.[[167]](#footnote-167)

Подводя итоги, следует отметить, что Конвенция Совета Европы, несмотря на множество очевидных плюсов, имеет несколько минусов, например, необходимость обращения к толкованию Пояснительного Доклада для уточнения содержания таких норм, содержание норм, которые потенциально могут ущемлять права человека либо суверенитет государств. Также, как указывалось ранее, часть государств отказывается от подписания данной Конвенции ввиду несоответствующих их интересам процессуальных аспектов. На настоящий момент Конвенция Совета Европы о киберпреступлениях 2001 г. является единственным международным договором, регулирующим международные аспекты сотрудничества в сфере киберпреступлений, охватывающий наибольшее количество государств-участников.

## Европейский Союз

Европейский Союз (далее – ЕС) высоко оценил работу Совета Европы. Учитывая тот факт, что большинство членов ЕС стали участниками Конвенции Совета Европы, потребность в гармонизации соответствующей отрасли законодательства практически отпадала. Несмотря на отсутствие единого документа, касающегося киберпреступлений, право ЕС изобилует различными нормативными актами, так или иначе связанными с компьютерными технологиями. В большинстве актов, фигурирует понятие «информационные системы», однако оно практически идентично понятию «компьютерные системы», используемые ООН и СЕ.

В Европейском Союзе в целом применяется идея «Электронной Европы» (eEurope),[[168]](#footnote-168) согласно которой каждый член общества должен стать частью информационного сообщества. «Электронная Европа» стала направлением в законодательстве Европейского Союза. Хотя концепция действует с 2005 года, до нее существовало множество рекомендаций, связанных с киберпространством в целом.[[169]](#footnote-169)

Исследуя правовые инструменты в рамках ЕС, следует обратить внимание на Рамочное решение Совета об атаках на информационные системы.[[170]](#footnote-170) Оно рассматривает общие вопросы сотрудничестве государств-Членов ЕС, а также затрагивает материальное уголовное право.[[171]](#footnote-171) В состав национального законодательства, согласно Рамочному Решению, должны быть включены следующие преступления: незаконный доступ к информационным системам,[[172]](#footnote-172) незаконное вмешательство в информационную систему,[[173]](#footnote-173) незаконное вмешательство в данные,[[174]](#footnote-174) и устанавливает ответственность за подстрекательство, помощь и пособничество в совершении таких преступлений. Составы преступлений, касающиеся персональных данных, были впервые определены, несмотря на существующую Конвенцию Совета Европы о защите индивидов в области автоматической обработки персональных данных, участниками которой также является большинство участников Европейского Союза.[[175]](#footnote-175) Также устанавливается ответственностью юридических лиц, что связано с особенностями большинства правовых систем государств-членов ЕС.

Данное рамочное решение было заменено Директивной Европейского Парламента и Совета от 12 августа 2013 года об атаках против информационных систем и замещении Рамочного Решения Совета 2005/222/JHA. Директива, как документ, обязательный для имплементации государствами-участниками Европейского Союза, наиболее эффективно регулирует правоотношения в сфере киберпреступлений и отражает эффективное международное сотрудничество в этой сфере.

Создатели Директивы учли особую опасность, связанную с нападениями на критическую инфраструктуру.[[176]](#footnote-176) Несмотря на участие в Конвенции Совета Европы, между членами Европейского Союза также существуют различия в следственных процедурах и материальном праве. [[177]](#footnote-177) И для целей эффективного сотрудничества в первую очередь в области пресечения терроризма и организованной преступности, Рамочное решение от 2005 года было «усовершенствовано» и приведено в соответствие с реалиями.

Директива содержит все те же составы киберпреступлений, указанные в Рамочном Решении: незаконный доступ к информационной системе, незаконное вмешательство в информационную систему, незаконное вмешательство в компьютерные данные. Однако, Директива включает некоторые новые составы: незаконный перехват компьютерных данных[[178]](#footnote-178) и использование компьютерных устройств для совершения преступлений.[[179]](#footnote-179) Также обновлены правила осуществления юрисдикции над киберпреступлениями. Если ранее юрисдикция ограничивалась только активным персональным и территориальным принципами, то в Директиве раскрыта возможность установления юрисдикции над лицом, которое имеет место жительства в государстве или лицом, чьи действия были направлены на получение выгоды юридического лица, организованного на территории государства. Также, как было указано ранее, авторы Директивы не прошли мимо преступлений против критической инфраструктуры, за совершение которых государствами-участниками должно быть установлено максимальное наказание не менее 5 лет лишения свободы.[[180]](#footnote-180)

На настоящий момент, данная Директива является основным международно-правовым инструментом, рассматривающим отдельно киберпреступления на территории Европейского Союза. Тем не менее, существует множество иных нормативных актов, связанных с реализацией и поддержкой указанной Директивы. В частности, это Директива об электронной коммерции,[[181]](#footnote-181) Директива о сохранении данных, созданных или обработанных с предоставлением публичных электронных сообщений или публичных сетей связи[[182]](#footnote-182) (которая успела стать предметом спора в Суде ЕС),[[183]](#footnote-183) Директивы о Персональных данных,[[184]](#footnote-184) и иные. Конкретно вопросов киберпреступлений также касается Рамочное Решение о предотвращении и урегулировании конфликта юрисдикции в уголовном судопроизводстве,[[185]](#footnote-185) которое рассматривает вопросы межгосударственного урегулирования суверенитета. Однако, вновь обращаясь к утверждению, что в киберпространстве нет суверенитета государств, общие процессуальные нормы вряд ли будут эффективны для преследования лиц за совершение киберпреступлений.

## СНГ

Государства – участники заключили соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации в 2001 году.[[186]](#footnote-186)

В отличии от Конвенции Совета Европы, Соглашение не столь часто упоминается в правовой литературе. Также, Соглашение кардинально отличается терминологически и содержательно от указанной Конвенции.

Во-первых, Соглашение обращается только к компьютерной информации. В качестве составов преступлений, Соглашение перечисляет неправомерный доступ и изменение данных, создание и распространение вредоносных программ, нарушение правил эксплуатации ЭВМ, незаконное использование программ и баз данных. Этот список вызывает определенные вопросы, в частности касающиеся нарушений правил эксплуатации ЭВМ. Что именно имели авторы Соглашения, не представляется ясным, что для эффективности Конвенции представляет достаточный недочет.

Касательно процессуальных вопросов, Соглашение устанавливает несколько форм сотрудничества, например, обмена информацией, исполнение запросов о проведение оперативно-розыскных мероприятий в соответствии с международными договорами, и иные. Следует отметить, что две вышеуказанные формы являются имеющими некоторую правовую значимость, в то время как остальные – подготовка кадров, обмен правовыми актами и иные, - являются в большей степени политическими или рекомендательными.

Также, Соглашение подробно описывает форму запроса об оказании содействия, порядок его исполнения. Представляется логичным, что такой международный договор имеет больше схожих черт со стандартным договором о сотрудничестве, нежели специальным договором, который имел бы особое влияние на становление международного сотрудничества в сфере борьбы с киберпреступлениями.

Исходя из вышеизложенного, следует отметить практическую ограниченность применения таких международно-правовых инструментов. Во-первых, это территориальная применимость: количество участников всех трех международных договоров ограничено и не охватывает практически половины существующих государств. Во-вторых, затруднена практическая применимость реализации таких договоров ввиду их прямой зависимости с институтом экстрадиции преступников, в большинстве случаев закрепленным в отдельных международных договорах. В-третьих, непосредственное использование процессуальных норм во всех трех случаях существенно затрагивает вопросы суверенитета государства, что может представляться достаточно нежелаемым при применении международного договора. Так или иначе, международно-правовое регулирование сотрудничества как стран СНГ, так и иных государств, представляется недостаточным в этом вопросе, как с позиции субъектного состава участников, участвующих в этом сотрудничестве, так и с позиции непосредственно договоров, поскольку их количество представляется удручающим, а сфера их действия зачастую представляется ограниченной.

Специальное регулирование не является всеобъемлющим. Отсутствует унифицированное регулирование, количество участников существующих международных договоров не охватывает даже половины существующих государств. Следует отметить, что международно-правовое сотрудничество должно строиться на основе общего понимания киберпреступления, а не на отдельных его разновидностях, тенденция развития таких договоров. Несмотря на различия в понимании киберпреступления, развитие отдельных его видов будет препятствовать дальнейшему сотрудничеству на этом поле. В связи с этим можно предположить, что создание всеобъемлющего международного договора, охватывающего общие аспекты киберпреступлений, является наиболее предпочтительным.

# 3. Проблемы реализации международно-правового сотрудничества в сфере борьбы с преступлениями, совершенными с использованием компьютерных технологий

Международно-правовое сотрудничество осложняется несколькими элементами, связанными со спецификой преступлений, совершаемых с использованием компьютерных технологий. В частности, это разграничение юрисдикции над преступлениями, связанными с трансграничным осуществлением такого преступления и применение материального права государствами после определения юрисдикции.

## 3.1 Разграничение юрисдикции государств в отношении киберпреступлений

Как неоднократно указывалось ранее, в киберпространстве нет границ, территории, оно является «виртуальным»,[[187]](#footnote-187) и применение понятия «суверенитет», соответственно, представляется достаточно проблематичным.

Предполагается, что киберпространство представляет собой нечто схожее с космосом или открытым морем,[[188]](#footnote-188) однако даже там существуют так называемые «квази-территории»: корабли под флагом государства, космические корабли определенных государств. Но так или иначе, такое пространство имеет физическое воплощение, в то время как киберпространство невозможно измерить или делимитировать.

Вопрос о реализации государственного суверенитета является одним из наиболее спорным в вопросе регулирования киберпространства. В частности, попытки регулирования киберпространства предпринимались ICANN (Internet Corporation for the Assiggned Numbers and Names),[[189]](#footnote-189) первоначально занимавшейся регистрацией доменных имен, а в дальнейшем занимающейся попытками кодификации и регулирования структуры в сети Интернет. ICANN является юридическим лицом по праву США, что вызывает у большинства государств и международных организаций сомнения в доверии к его регулированию.

Если с позиции структурирования регулирование осуществляется ICANN, то вопросы электросвязи и киберинфраструктуры регулирует Международный союз электросвязи, учрежденный в соответствии с Международной Конвенций электросвязи. Одной из целей МСЭ было обеспечение и расширение международного сотрудничества с целью усовершенствования и рационального использования всех видов электросвязи. Так подлежат регулированию аспекты технического обеспечения деятельности киберинфраструктуры, будь то радиочастотный спектр, помехи, структуру кибербезопасности и иные.

Но вышеуказанные организации осуществляют только частичное регулирование базовых аспектов киберпространства, создающих доступ к нему, в то время как власть государства в киберпространстве остается практически неурегулированным. Во-первых, некоторые сайты, то есть комплексы данных в киберпространстве, образующие «площадку», не попадают под юрисдикцию государств. Изначально представлялось, что юрисдикция государств распространяется на соответствующие домены, составляющие определенный сегмент Интернета. То есть, регулирование домена .ru осуществляется Российской Федерацией, .ua – Украиной. Но возник вопрос о регулировании других доменов, не имеющих территориальной привязки, а также доменов, которые входят в зону Darknet.

Во-вторых, если учитывать, что киберпространство не является материальным, «реальным», тогда при совершении киберпреступления отсутствует место преступления. Единственным идентификатором места выступает TCP/IP адрес, который отражает сетевой адрес узла в компьютерной сети и является уникальным. Однако, несколько сайтов могут использовать один IP адрес, а пользователи могут пользоваться различными способами для сокрытия или подмены такого идентификатора.

В контексте рассматриваемой темы, следует проанализировать виды юрисдикции, применимой в киберпространстве.

Обычно выделяют четыре принципа, в соответствии с которыми осуществляется юрисдикция: территориальный принцип, принцип эффекта, персональный принцип и защитный принцип. Их же иногда классифицируют как активный и пассивный территориальный и персональный принципы.

Основным принципом юрисдикции является территориальный принцип, применяемый большинством государств.[[190]](#footnote-190) Но в случае киберпреступлений, достаточно сложно установить место совершения преступления. Можно выдвинуть несколько вариантов: местонахождение непосредственно преступника, серверов пользователей, на компьютерные системы которых было направлено деяние, либо

Одним из широкоприменяемых видов юрисдикции является активная персональная: юрисдикция государства определяется по национальности лица.[[191]](#footnote-191) Она же применяется в большинстве государств при определении юрисдикции над киберпреступлениями.[[192]](#footnote-192)

Наиболее известным делом о киберпреступлениях, в котором осуществлялся принцип активной персональной юрисдикции, хотя и над юридическим лицом, является дело Зиппо, рассматриваемое судом Западного региона Пенсильвании США.[[193]](#footnote-193) Заявитель – Компания Зиппо, производящая всемирно известные зажигалки, обвинила Зиппо Дот Ком – калифорнийскую корпорацию, которая управляла сайтами под доменными именами, схожими по названию с компанией. Однако, суд отказал в рассмотрении дела, указав, что он не обладает юрисдикцией над Зиппо Дот Ком, поскольку у организации в целом отсутствуют какие-либо связи с Пенсильванией, в частности суд отметил, что юрисдикция должна определяться при анализе интерактивности и коммерческого характера обмена информации, производимой на сайте.[[194]](#footnote-194) В дальнейшем, практика судов США расширилась, в частности, устоялся критерий «скользящей шкалы», в соответствии с которой выделяются три группы сайтов: активные сайты, используемые для ведения бизнеса, интерактивные и пассивные сайты, при определении юрисдикции над которыми следует учитывать фактор, указанный в деле Зиппо.

Поскольку в киберпреступления в большинстве случаев совершаются трансгранично, возможно применение двух принципов экстерриториальной юрисдикции - субъективного и объективного.

Субъективный территориальный принцип, предполагает в качестве основы определения юрисдикции место совершения преступления вне зависимости от того, в каком государстве будут эти последствия. Объективный территориальный принцип, включающий в себя защитную юрисдикцию (пассивный территориальный принцип), в свою очередь, основан на последствиях этого преступления.[[195]](#footnote-195)

Пассивный персональный принцип представляет собой осуществление юрисдикции государством при совершении преступлений против его граждан. В частности, такая юрисдикция осуществляется США: при совершении теракта, жертвами которого стали граждане США, исполнительные органы власти вправе расследовать это преступление.[[196]](#footnote-196) Пассивный территориальный принцип применяется в случае наличия эффекта на территории государства при совершении преступления, если таковое было совершено за его пределами.[[197]](#footnote-197) Он применяется Международным Уголовным Судом.[[198]](#footnote-198)

В деле «СС Лотус», Постоянная Палата международного правосудия при рассмотрении вопроса о наличии турецкой юрисдикции над французским капитаном при столкновении двух пароходов, постановила, что даже если основным видом юрисдикции является территориальная юрисдикция, при отсутствии запрета на осуществление такой юрисдикции, государство свободно в ее определении в соответствии с нормами международного права,[[199]](#footnote-199) и, поскольку последствия столкновения произошли на территории турецкого парохода, Турция имеет право осуществлять юрисдикцию над гражданином Франции.[[200]](#footnote-200)

При определении юрисдикции возникают множество вопросов, связанных с должной реализацией уголовного преследования.

Первый способ, субъективный, кажется наиболее традиционным, учитывая фактическое включение в него активного персонального и территориального видов юрисдикции. Однако, возникает несколько вопросов: сможет ли (и захочет ли?) государство определить конкретного преступника, хватит ли у него возможностей уголовного процесса для этого, присутствует ли соответствующее уголовное законодательство, и, в результате, сможет ли государство должны образом привлечь преступника к ответственности? Следует отметить тенденцию наличия группировок киберпреступников, активно поощряемых или даже покровительствуемых государством, которая усугубляет вопрос эффективного уголовного преследования за киберпреступления. Такой способ установлен в Конвенции Совета Европы о киберпреступлениях 2001 г.

Однако второй способ реализации юрисдикции так же представляется спорным. Во-первых, возникает вопрос о практической реализации преследования. Выдаст ли государство своего гражданина для уголовного преследования, будет ли лицо экстрадировано? Во-вторых, будет ли расследование киберпреступления соответствовать гарантиям прав человека? В-третьих, в соответствии с каким правом следует рассматривать дело о киберпреступении?[[201]](#footnote-201) Формально, преступник, гражданин государства, на территории которого он и совершал преступление, не выходил из комнаты и рассчитывал на то, что к нему будут применены нормы другого государства. Такой способ использовался в большинстве дел, рассматриваемых судами США в конце XX века.[[202]](#footnote-202)

Так как оба способа осуществления юрисдикции осложнены объективными сомнениями в их реализации, некоторые исследователи предлагают использовать универсальную юрисдикцию.

Универсальная юрисдикция – еще один вид юрисдикции, который может быть использован любым государством за любое серьезное нарушение права вне зависимости от места совершения преступления или гражданства преступника.[[203]](#footnote-203) В деле Йеродия, Международный Суд ООН постановил, что осуществление юрисдикции Бельгией над гражданином Конго, который принимал участие в геноциде в Руанде, является незаконным, в связи с чем идея о применении универсальной юрисдикции была отвергнута.[[204]](#footnote-204) Тем не менее, при совершении киберпреступлений вопрос о применении универсальной юрисдикции возникает вновь как альтернатива стандартным видам юрисдикции. Но универсальную юрисдикцию также можно подвергнуть критике. Вероятно, определенные преступления, имеющие наиболее серьезные последствия, в частности кибертерроризм, могут преследоваться на основании универсальной юрисдикции, в то время как применение такого принципа к остальным киберпреступлениям будет практически невозможным и только еще больше усугублять споры, касающиеся конфликта юрисдикций.[[205]](#footnote-205)

Конвенция Совета Европы о киберпреступлениях 2001 г. устанавливает порядок осуществления юрисдикции: государство может осуществлять юрисдикцию на основании активного территориального принципа либо активного персонального принципа.[[206]](#footnote-206) Однако строгого разделения юрисдикции государств в случае их конфликта не предусмотрено, хотя указано, что государства должны сотрудничать друг с другом по этому поводу.

Разумным было предложение, содержащееся в Стэнфордский проект Конвенции о защите против Киберпреступлений и кибертерроризма 2000 г. В первую очередь право осуществления преследования принадлежит государству, на территории которого находится преступник. Если это государство решает не осуществлять юрисдикцию над этим преступлением, другие государства в следующем порядке могут осуществлять юрисдикцию:

- государства, на чьей территории преступлением нанесен существенный ущерб (в соответствии с принципом эффекта),

- государство, гражданином которого является преступник (активный персональный принцип),

- любое государство, где может быть обнаружен этот преступник,

- любое государство с разумными основаниями для юрисдикции.[[207]](#footnote-207)

Вопрос осуществления юрисдикции является ключевым при международном сотрудничестве в сфере киберпреступлений, поскольку именно по правилам юрисдикции будет осуществляться преследование. Однако, разногласия в различиях применения юрисдикции являются кардинально противоположными и затрудняющими любое взаимодействие между государствами в этой области.

Наряду с Конвенцией Совета Европы о киберпреступлениях 2001 г., Стэнфордский Проект устанавливает такой порядок осуществления юрисдикции, но в отличие от указанной, не является международным договором и не имеет обязательной силы. Тем не менее, предложения Стэнфордского проекта на настоящий момент являются наиболее рациональными, и разрешают вопрос юрисдикции, в то время как существующие международные инструменты не могут определить порядок осуществления юрисдикции государства. В связи с чем, следует сделать вывод, что положения Стэнфордского проекта следует учитывать при создании международных договоров, связанных с киберпреступлениями.

Урегулирование вопросов юрисдикции является первоначальным при сотрудничестве государств в данном вопросе. Свобода выдачи граждан для их преследования в другом государстве остается свободой усмотрения государств в части реализации собственной юрисдикции, что осложняет в целом расследование и раскрытие преступлений, совершенных в киберпространстве. И указание на прямой порядок реализации значительно облегчит порядок сотрудничества государств. Несомненно, множество процессуальных моментов достаточно сложно урегулировать в рамках ООН, однако регулирование в части определения киберпреступлений, определения порядка осуществления юрисдикции и минимальных стандартов осуществления сотрудничества в процессуальном аспекте является наиважнейшим в сотрудничестве в борьбе с преступлениями, совершенными с использованием компьютерных технологий.

## 3.2 Национальное право государств, применимое к определению киберпреступлений.

Поскольку вопросы юрисдикции при сотрудничестве в сфере борьбы с киберпреступлениями не урегулированы, следует проанализировать национальное законодательство, которое будет непосредственно регулировать непосредственно киберпреступления.

На практике существует проблема определения применимого материального права. Киберпространство, как новое поле деятельности, может отражать практически идентичные реальной жизни преступления – кражу, мошенничество, но может способствовать созданию новых видов преступлений, имеющих исключительную связь с компьютерными технологиями.

Международный союз электросвязи разделяет киберпреступления на преступления против конфиденциальности, неприкосновенности и доступности компьютерных данных или систем, преступления, связанные с контентом, преступления, связанные с интеллектуальной собственностью и преступления, связанные с компьютерными системами[[208]](#footnote-208)

Один из наиболее авторитетных экспертов в области киберправа, Давид С. Уолла, профессор Даремского университета (Великобритания), разделяет все киберпреступления на 3 вида: преступления против неприкосновенности компьютера, преступления, совершаемые с использованием компьютеров, преступления, связанные с контентом.[[209]](#footnote-209) К первым он относит DDos – атаки, преступления, направленные на взлом систем и выведение их из строя, ко вторым – уже существующие преступления, которые совершаются с помощью компьютерных систем. К третьим – hate speech, шпионаж, преступления против персональных данных, совершаемые непосредственно в киберпространстве.[[210]](#footnote-210) Несмотря на такую классификацию, к сожалению, в большинстве исследований и национальной практике такое разделение не учитывается.

Такая классификация уместна ввиду необходимости применения классификации конкретных составов на национальном уровне. Нормы национального права при их применении не должны терять той цели, на защиту которой они направлены.

1. Преступления против конфиденциальности, неприкосновенности и доступности компьютерных данных и систем.

Одним из наиболее опасных преступлений в данной категории является вмешательство в компьютерную систему.[[211]](#footnote-211) Ярким примером таких преступлений являются DDos – атаки.[[212]](#footnote-212) Это действия, направленные на «отказ в обслуживании»; атаки направлены на невозможность обслуживания целевым компьютером авторизированных пользователей.[[213]](#footnote-213) Преступники используют «зомби-компьютеры», которые подконтрольны злоумышленнику без ведома их пользователей. Многочисленное отправление запросов выводит из строя сервера, в связи с чем обслуживание им пользователей прекращается. Использование способов Smurf или Fraggle приводит практически к 100% отказу в обслуживании.[[214]](#footnote-214) Одним из наиболее распространенных видов такой атаки является перегруз компьютерной системы, последствия чего могут быть различными – от кратковременного отказа системы до физического уничтожения киберинфраструктуры в силу перегруза.

Особая опасность данного вида преступления была отмечена большинством государств. В связи с распространением DDos - атак, Великобритания в 2006 году внесла изменения в законодательство: акты, которые составляют незаконный акт по отношению к компьютеру, в то время, когда целью такого действия было предотвращение или помеха доступа к любой программе или компьютеру, либо ослабить выполнение программой какой-либо операции, ибо ослабить выполнение компьютером каких-либо задач, представляют собой преступление.[[215]](#footnote-215) Законодательство Канады предусматривает более обширную формулировку: преступление должно иметь целью «совершение действий, причиняющих вред обществу».[[216]](#footnote-216) Австралийское законодательство[[217]](#footnote-217) включает практически все вышеуказанные составы преступлений, формулировки закона позволяют расширительно толковать данные составы и термины.

В данную группу также могут быть включены преступления, связанные с вирусами и вредоносным программным обеспечением.

Вирусы могут иметь множество назначений: от слежки до выведения из строя оборудования. Одним из известнейший является вирус Stuxnet, результатом которого стало практически полное выведение иранского ядерного реактора из-под контроля. Вредоносное программное обеспечение имеет своей целью преимущественно частные компьютерные системы, однако их назначение также различно.

Незаконный доступ также посягает на конфиденциальность и неприкосновенность данных. В литературе можно также встретить определение «hacking» (хакинг), ассоциируемый с незаконным доступом. Незаконный доступ признан незаконным в большинстве государств, а также фигурирует как состав преступления в Конвенции Совета Европы о киберпреступлениях.[[218]](#footnote-218) Зачастую, в состав этого преступления относят компьютерный шпионаж.[[219]](#footnote-219) Шпионаж имеет множество форм: кейлоггинг, использование сканирования незащищенных данных, и т.д.

Пограничным преступлением является незаконный перехват информации,[[220]](#footnote-220) основанный на перехвате исключительно информации, либо путем проникновения в компьютерную систему, либо путем перехвата коммуникационной инфраструктуры. Перехват представляет собой наблюдение и изъятие информации без каких-либо взаимодействий с отслеживаемой информацией.[[221]](#footnote-221) В отличие от перехвата, вмешательство в данные представляет собой взаимодействие с информацией, будь то ее уничтожение, модификация или запрет к ее доступу. В большей части случаев совершения такого преступления, вмешательство имеет финансовый интерес.

1. Преступления, связанные с контентом.

Настоящая группа преступлений содержит преступления, составы которых уже известны национальному праву, но могут совершаться путем применения компьютерных технологий и связаны с содержащейся информацией.

К таким преступлениям относятся hate speech, распространение ксенофобных материалов[[222]](#footnote-222) и оскорбление религиозных символов.[[223]](#footnote-223) Также к ним относят преступления, связанные с эротическими или порнографическими материалами[[224]](#footnote-224) и, отдельно, детскую порнографию. Если дифференциация различных составов, касающихся первого вида преступлений, представляется естественной, то вторая категория должна быть отнесена к преступлениям международного характера. Отдельной категорией преступлений данной группы являются преступления, связанные с онлайн играми.[[225]](#footnote-225)

Преступления, связанные с контентом, включают в себя деяния, связанные с информацией: спамом, клеветой, раскрытием конфиденциальной информации, и иные. [[226]](#footnote-226)

1. Преступления, связанные с интеллектуальной собственностью.

Наиболее распространенным преступлением в Интернете является пиратство. Незаконное распространение копий продуктов представляет собой всемирную проблему, однако такой вопрос в большинстве случаев не может быть разрешен окончательно: при наличии копий в реальном мире их можно уничтожить физически, в то время как количество копий в Интернете стремится к бесконечности. Субъекты авторского права встречаются с непреодолимой проблемой, связанной с торрент-сервисами, пользователи которых имеют часть каждого продукта, раздавая их другим пользователям, в то время как сайты обладают лишь хеш-суммой, не представляющей собой цельного файла.

В виду огромного количества сайтов, существует проблема, связанная с торговыми марками или доменными именами, выражающаяся в использовании таковых для противозаконных целей.[[227]](#footnote-227)

4) Преступления, связанные с компьютерными системами.

К числу таких преступлений относят мошенничество,[[228]](#footnote-228) кражу, злоупотребление устройством[[229]](#footnote-229) и даже фальшивомонетничество.

Киберкража и мошенничество стали одним из наиболее частых преступлений. Кража средств с кредитных карт, с онлайн-сервисов совершаются повсеместно. Однако, причинами кражи могут быть совершенно разные предпосылки: ложные представления о сервисе, раскрытие информации, злоупотребление должностными обязанностями или просто обман.

Киберпространство представляет множество вариантов для совершения киберкражи. Самый грубый вид такой кражи представляет собой взлом банковских систем и переводы.

Мошенничество предполагает большее человеческое участие в таких преступлениях. Например, известные «Нигерийские письма», «русская афера», мошенничества с кредитными картами, мошенничества с онлайн-системами и эскроу.[[230]](#footnote-230) Выделяют множество объектов мошенничества в киберпространстве: от кредитных карты до банковских данных.[[231]](#footnote-231)

Вместе с этим, применяется также кража личности[[232]](#footnote-232) – один из видов преступлений, направленный на получение данных - от персональных до физиологических, которые используются в качестве идентификатора в некоторых системах.[[233]](#footnote-233) Кража таких данных провоцирует ряд новых преступлений, таких как создание фальшивых документов.

Преступления, совершаемые с использованием компьютерных технологий совершаются различными способами и плотно вошли в жизнь современного общества. Существуют и иные, не перечисленные в данном разделе преступления, которые являются составными, либо относятся преступлениям международного характера, что будет раскрыто далее. Массив преступлений, включенных в национальное законодательство государств, варьируется в зависимости от различных факторов, одним из которых является участие в международных договорах или международное сотрудничество в рамках региональных организаций. Тем не менее, анализ подобных преступлений позволяет рассмотреть киберпреступления в практико-ориентированной среде: несмотря на множество угроз, государства пытаются совершенствовать свое законодательство тем или иным образом.

Преступления, совершаемые с использованием компьютерных технологий совершаются различными способами и плотно вошли в жизнь современного общества. Существуют и иные, не перечисленные в данном разделе преступления, которые являются составными, либо относятся преступлениям международного характера, что будет раскрыто далее. Массив преступлений, включенных в национальное законодательство государств, варьируется в зависимости от различных факторов, одним из которых является участие в международных договорах или международное сотрудничество в рамках региональных организаций. Тем не менее, анализ подобных преступлений позволяет рассмотреть киберпреступления в практико-ориентированной среде: несмотря на множество угроз, государства пытаются совершенствовать свое законодательство тем или иным образом.

Подводя итоги, следует отметить, что подходы к определению юрисдикции непосредственно влияет на применение того или иного материального права, которое также значительно различается. Следует сделать вывод о том, что в результате подобных разногласий представляется затруднительным унифицировать как понятие киберпреступления, так и достигнуть консенсуса в вопросе определения порядка осуществления юрисдикции.

# Заключение

Гипотеза, поставленная в начале исследования, состояла в предположении о недостаточности международно-правового регулирования сотрудничества в сфере преступлений, совершенных с использованием компьютерных технологий.

В ходе исследования были определены и рассмотрены следующие проблемы:

- отсутствие универсального определения «преступления, совершенного с использованием компьютерных технологий», препятствующее эффективному международному сотрудничеству в сфере борьбы с преступлениями, совершенными с использованием компьютерных технологий;

- частичная применимость норм общего международного права к киберпреступлениям;

- отсутствие универсального международного договора в сфере киберпреступлений, определяющего общие подходы к регулированию преступлений, совершенных с использованием компьютерных технологий;

- различные и несогласуемые подходы к определению юрисдикции над рассматриваемым видом преступлений;

- различное материальное право государств, применимое к преследованию киберпреступлений и выделяющее множество различных видов преступлений.

В качестве результата следует определить следующие выводы:

- преступление, совершаемое с использованием компьютерных технологий, представляет собой незаконное деяние, совершаемое в киберпространстве и направленно против компьютерных систем, компьютерных данных, либо совершенное с использованием компьютерной системы. Данное понятие является наиболее общим, но государства применяют множество иных, различных и несовпадающих терминов, что исключает эффективное международное сотрудничество в данной сфере.

- регулирование, существовавшее до развития киберпреступлений, лишь частично затрагивает киберпреступления. Существующие международные конвенции не включают в сферу действия большинство преступлений, совершаемых с киберпространстве. Также представляется проблемным то, что что некоторые государства не желают приравнивать преступления в киберпространстве к преступлениям, которые происходят в «реальном мире», применение вышеуказанных норм затрудняется различными подходами к такой проблеме.

- Государства различают множество видов юрисдикции, однако вопрос юрисдикции является наиболее важным в осуществлении международного сотрудничества в сфере киберпреступлений, поскольку порядок осуществления преследования преступлений, совершенных с использованием компьютерных технологий, является первоначальным при вопросе расследования таких преступлений ввиду их трансграничного характера.

- Массив преступлений, включенных в национальное законодательство государств, варьируется в зависимости от различных факторов, одним из которых является участие в международных договорах или международное сотрудничество в рамках региональных организаций. Тем не менее, вопрос материального права представляет проблемный вопрос, поскольку при осуществлении преследования, государства могут применять различные составы преступлений, что будет значительно осложнять международное сотрудничество в борьбе с преступлениями.

Таким образом, гипотеза, установленная в начале исследования, таким образом, была подтверждена.

Вышеуказанные проблемы могут быть разрешены путем создания специального международного договора, в который будут включены положения о материальном праве, содержащие минимальный консенсус в рассматриваемой сфере, положения о минимальных процессуальных стандартах, касающихся экстрадиции и помощи в процессуальном аспекте, а также положения, устанавливающие порядок определения юрисдикции над рассмотренными видами преступлений.

**Международные нормативно-правовые акты и международная судебная практика**

Устав ООН // 1 UNTS XVI, 26 июня 1945.

Конвенция о психотропных веществах // U.N.T.S. 1019, 1971.

Единая конвенция о наркотических средствах 1961 года с поправками, внесенными в нее в соответствии с Протоколом о поправках к Единой конвенции о наркотических веществах 1961 года // U.N.T.S. 976, 1975.

Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ // U.N.T.S.1582, 1988.

Римский Статут // A/CONF.183/9, 17 июля 1998, U.N. T. S, vol. 2187, No. 38544.

Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии // Резолюция Генеральной Ассамблеи 54/263, 25 мая 2000, U.N.T.S. 2173.

Конвенция Организации Объединенных Наций против транснациональной организованной преступности // General Assembly Resolution 25, annex I, 55th Sess., U.N. Doc. A/45/49, Vol. I, 2001.

Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) [Электронный ресурс] : // РЕЖИМ ДОСТУПА : <http://www.cis.minsk.by/>

Международная конвенция о борьбе с финансированием терроризма // Резолюция Генеральной Ассамблеи 54/109, прил. 1, 54 Сессия, U.N.T.S. 2178.

1. The case of the S.S. “Lotus” // Permanent Court of the International Justice, 7 September 1927, Publication of the Permanent Court of International Justice, Series A, No. 10.
2. Statute of the Council of Europe // European Treaty Series, Nos 1/6/7/8/11, 5 May 1949.
3. Nottebohm Case (Liechtenstein v. Guatemala), (Second Phase) // ICJ Reports, 1955.
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // European Treaty Series, No. 108, Strasbourg, 28 January 1981.
5. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // OJ L 281, 23.11.1995.

Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01) // The Council of the European Union, OJ C 329 , 04/11/1996.

1. Draft Code of Crimes against the Peace and Security of Mankind with commentaries // Yearbook of the International Law Commission. 1996. Vol. II, Part Two.

Decision No CM/Del/Dec(97)583 // 4 February 1997, Committee of Ministers (The Committee of Experts on Crime in Cyber-space).

1. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // OJ L 024 , 30/01/1998.

Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC) // The Council of the European Union, OJ L 270, 7.10.1998.

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market // OJ L 178 , 17/07/2000
2. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series . 2001. No. 185.
3. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185.
4. eEurope 2005: An information society for all, COM (2002) 263 // Commission of The European Communities, Brussels, 2002.

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems // European Traty Series. No.189. 2003

Amendment to the Rome Statute of the International Criminal Court on the Crime of Aggression, articles 8bis, 15bis and 15ter, 11 June 2010 [Electronic Resource] // Resolution RC/Res.6 of 11 June 2010. Art. 8-bis. РЕЖИМ ДОСТУПА : <https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf>

1. Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium) // ICJ Reports, 2002.

Council Framework Decision of 24 February 2005 on attacks against information systems (2005/222/JHA) // The Council of European Union, OJ L 69, 16.3.2005.

1. Directive 2006/24/EC o The European Parliament and of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC // OJ L 105/54 13 April 2006.

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceeding // OJ L 328/42, 15 December 2009

1. Combating the sexual abuse and sexual exploitation of children and child pornography, Directive 2011/93/EU // OJ L 335 of 17.12.2011.
2. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // OJ L 218, 14 August 2013
3. Halford v. UK // ECtHR, App. N 20605/92, 25 June 1997.

Ireland v. European Parliament and Council of the European Union // 10 February 2009, C-301/06, ECLI:EU:C:2009:68.

1. Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, STL-11-01/I // Special tribunal for Lebanon, Appeals Chamber, 16 February 2011Recommendation No. R (89) 9 of the Committee of Ministers to Member Stares on Computer-related Crime // Council of Europe, Committee of Ministers, 13 September 1989, 428th meeting of the Ministers’ Deputies.

Recommendation No. R (95) 13 // Council of Europe, Committee of Ministers, 11 September 1995, 543rd meeting of the Ministers’ Deputies.

1. Rome Statute of the International Criminal Court // A/CONF.183/9, UN General Assembly, 17 July 1998.
2. Zakharov v. Russia // ECtHR, App. N 47143/06, 4 December 2015.

**Национальные нормативно-правовые акты и иные официальные документы**

1. Act to combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence [Electronic Resource] : Chapter 08:06, Cybercrime and Computer Related Crimes, Government of Botswana, 28 December 2007. - Режим доступа : <http://www.bocra.org.bw/sites/default/files/documents/CHAPTER%2008-06%20CYBERCRIME%20AND%20COMPUTER%20RELATED%20CRIMES.pdf>
2. Advisory Report on the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999 / House of Representatives, Standing Committee on Legal and Constitutional Affairs // Parliament of the Commonwealth of Australia, 2000.
3. Anti-Cyber Crime Law, Royal Decree No. M/17 8 Rabi 1 1428 [Electronic Resource] : 26 March 2007, Kingdom of Saudi Arabia. Режим доступа : <http://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf>

Antiterrorism and Effective Death Penalty ACT // 110 Stat. 1214

Commonwealth Cybercrime Initiative [Electronic Resouce] // The Commonwealth. Режим доступа : http://thecommonwealth.org/commonwealth-cybercrime-initiative

1. Computer Crime Act No. 24 of 2007 [Electronic resource] : 13 July 2007, Parliament of the Democratic Socialist Republic of Sri Lanka. Режим доступа : <http://www.slcert.gov.lk/Downloads/Acts/Computer_Crimes_Act_No_24_of_2007(E).pdf>
2. Computer Crimes Act 1997, Act 563 [Electronic Resource] : 30 June 1997, Parliament of Malaysia. Режим доступа : <http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20563.pdf> ;
3. Computer Misuse Act 1990 // 29 June 1990, United Kingdom Parliament.
4. Criminal Code // R.S.C., Parliament of Canada, 1985, c. C-46.
5. Criminal Code Act 1995, Act No. 12 // Commonwealth of Australia.
6. Criminal Code of the Republic of Bulgaria, Chapter Nine – A [Electronic Resource] : SG No 92/2003, Government of Republic Bulgaria. - Режим доступа : <http://www.vks.bg/english/vksen_p04_04.htm>

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) // The Parliament of Australia, 2004.

Cybercrime Act, 2007 [Electronic Resource] : 30 June 2007, National Council of Republic of Sudan. Режим доступа : <https://www.unodc.org/res/cld/document/sdn/2007/cybercrime_act_2007_html/Sudan_Cybercrime_Act_2007_EN.pdf>.

1. Cybersecurity law of the People's Republic of China // 7 November 2016, National People's Congress.
2. Electronic Communications and Transactions Act 25 of 2002 // 31 July 2002, Parliament of the Republic of South Africa.

Dutch Criminal Code [Electronic Resource] // Legislationline. Sec. 326c. Режим доступа : http://www.legislationline.org/documents/id/4693

German Penal Code // Federal Law Gazette, 1998.

Identity Cards Act 2006 // Parliament of the United Kingdom, 2006.

Law on Technology Transfer No. 80/2006/QH11 [Electronic Resource] : 25 December 2001, National Assembly of the Socialist Republic of Vietnam. Режим доступа : <http://www.wipo.int/edocs/lexdocs/laws/en/vn/vn050en.pdf>.

1. Law No. 2008-11 on Cybercrime [Electronic Resource] : National Assembly of Republic of Senegal, 25 January 2008. - Режим доступа : <http://www.wipo.int/edocs/lexdocs/laws/en/sn/sn008en.pdf>

Ley Especial Contra Los Delitos Informáticos [Electronic Resource] : 30 de octubre de 2001, La Asamblea Nacional De La República Bolivariana De Venezuela. - Режим доступа: <http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf>

Protection of Official Data: A Consultation Paper // Crown Copyright, London, 2017

1. Terrorism Act 2000 // 2000, Parliament of the United Kingdom.
2. The Information Technology Act No. 21 of 2000 [Electronic Resource] : 9 June 2000, Parliament of Republic of India. - Режим доступа: <http://meity.gov.in/writereaddata/files/itbill2000.pdf> ;
3. United States Code // 2012 ed., Supplement 1.
4. Unlawful Internet Gambling Enforcement Act of 2006 // 13 October 2006, 31 U.S.C.: Money and Finance
5. Attorney General v Makamian (Aram), Appeal Decision, Criminal Appeal No 258/06, ILDC 833 (CY 2007), 19th July 2007, Cyprus; Supreme Court [Sup Ct]; Supreme Court as Court of Appeal; Criminal Division
6. R v Gold, 1988, 1 AC 1063
7. R. v. Oliver and Others [2003] 2 Cr.App.R. (S) 64
8. R. v. Sharpe, 2001 SCC 2.
9. United States v. Hilton, 167 F.3d 61 (1st Cir. 1999),
10. United States v. Petersen 98 F.3d 502 (9th Cir., 1996).

Zippo Mfg. Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119

**Рекомендательные международные акты**

Доклад совещания Межсессионной межправительственной группы экспертов открытого состава для разработки предварительного проекта возможной всеобъемлющей международной конвенции против организованной транснациональной преступности (Варшава, 2-6 февраля 1998 года) // E/CN.15/1998/5, 18 февраля 1998, Экономический и Социальный Совет, ООН.

Определение агрессии // Резолюция Генеральной Ассамблеи 3314 (XXIX) от 14 декабря 1974, Официальные отчеты Генеральной Ассамблеи, двадцать девятая сессия, Приложение, № 31.

Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] // Сектор развития Электросвязи, Международный Союз Электросвязи. Режим доступа : <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf>

Рекомендация МСЭ-Т X.1205 (04/2008) [Электронный ресурс] // МСЭ, Сектор стандартизации электросвязи МСЭ, Серия Х: сети передачи данных, взаимосвязь открытых систем и безопасность: безопасность электросвязи. Режим доступа : <https://www.itu.int/rec/T-REC-X.1205-200804-I>

Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства [Электронный ресурс] // ОБСЕ, Вена: Ueberreuter Print GmbH, 2013. Режим доступа: http://www.osce.org/ru/secretariat/110472?download=true

1. Comprehensive Study on Cybercrime [Electronic Resource] : United Nations Office on Drugs and Crime, United Nations, New York, 2013. - Режим доступа: <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.
2. Consideration of Reports submitted by States Parties under the OPSC, Concluding Observations on Turkey, CRC/C/OPSC/TUR/CO/1 // United Nations Committee on the Rights of the Child, 9 June 2006.
3. Crimes related to computer networks : Background paper for the workshop on crimes related to computer network // A/CONF.187/10. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000.
4. Qatar National Cyber Security Strategy // May 2014, Ministry of Information and Communications Technology.
5. Report of the Transborder Group for 2013, T-CY (2013)30 // Ad-hoc Subgroup on Transborder Access and Jurisdiction, Cybercrime Convention Committee, Strasbourg, 5 November 2013
6. Schmitt, M. Tallinn Manual on the International Law Applicable to Cyber Warfare / NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

The use of the Internet for terrorist purposes [Electronic Resource] // United Nations Office on Drugs And Crime, UN, New York, 2012. Режим доступа : <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>

1. T-CY Guidance Note #1: On the notion of “computer system”, Article 1.a Budapest Convention on Cybercrime, T-CY(2012)21// Cybercrime Convention Committee, Strasbourg, 5 December 2012
2. T-CY Guidance Note #8: SPAM, T-CY(2014)20 // Cybercrime Convention Committee, Strasbourg, 3 December 2014
3. T-CY Guidance Note #11 (Draft) : Aspects of Terrorism covered by the Budapest Convention // Cybercrime Convention Committee, Council of Europe, Strasbourg, 4 October 2016
4. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. Режим доступа : <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>
5. United Nations Manual on the prevention and control of computer-related crime / International Review of Criminal Policy, United Nations publication, Sales No. E.94.IV.5. New York. 1994.
6. Wamala F. National Cybersecurity Strategy Guide 2011 [Electronic resource] / ITU, 2011. Режим доступа: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

**Доктринальные источники**

1. Верле, Г. Принципы международного уголовного права: учебник / пер. с англ. С.В. Саяпина. М.: ТрансЛит, 2011.
2. Марков, А. С. Цирлов, В. Л. Руководящие Указания по Кибербезопасности в Контексте ISO 27032 // Вопросы кибербезопасности. 2014. N 1(2).

Международное право. Особенная часть : учеб. для студентов юрид. фак. и вузов / И.И. Лукашук;

Международное право / Вольфганг Граф Витцтум [и др.] ; пер. с нем., 2-е изд. 2015.

Рос. акад. наук, Ин-т государства и права, Академ. правовой ун-т. — Изд. 3-е, перераб. и доп. — М. : Волтерс Клувер, 2005.

1. Подготовительные материалы, касающиеся переговоров о разработке Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Протоколов к ней / Управление Организации Объединенных Наций по наркотикам и преступности, ООН, Нью-Йорк, 2006.
2. Ansari. N., Shevtekar A.,On the new breed of Denial of Service (DOS) attacks in the Internet // Saadawi, T. N., Jordan, L., & Army War College, Cyber infrastructure protection. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011.
3. Baranetsky, V. What is cyberterrorism? Even experts can’t agree [Electronic Resource] // The Harvard Law Record, 5 November 2009. Режим доступа : <http://hlrecord.org/2009/11/what-is-cyberterrorism-even-experts-cant-agree/>
4. Bassiouni, M. C. International Criminal Law. Transnational Publishers, Inc., Ardsley, 1999.
5. Benson, M. L., Simpson S, S. White-Collar Crime: An Opportunity Perspective / New York: Routledge, 2009.
6. Boister N., Currie R.J. Routledge Handbook of Transnational Criminal Law. Routledge, 2015.
7. Bowker, A. Cybercrime Handbook for Community Corrections: Managing Offender Risk in the 21st Century // Charles C Thomas Pub Ltd, 2012.
8. Brownlie, I. Principles of public international law // 7th(ed), Oxford University Press, 2008.

Cassese, A. International Criminal Law // 2nd ed., Oxford University Press, 2008

1. Choo, K.-K. R., Grabosky, P. Cyber Crime // L. Paoli, Oxford Handbook of Organized Crime. Oxford: Oxford University Press, 2013. DOI: 10.1093/oxfordhb/9780199730445.013.003.
2. Conway, M., Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures: Working Papers in International Studies // Centre for International Studies, Dublin City University, 2008.
3. Crawford J., Brownlie I. Brownlie's principles of public international law. 8th ed. Oxford: Oxford University Press, 2012.

Denning, D. Testimony before the Special Oversight Panel on Terrorism // Committee on Armed Services, U.S. House of Representatives, 2000.

Financial Coalition Against Child Pornography : Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography [Electronic Resource] : 1 February 2011, Financial Coalition Against Child Pornography. Режим доступа : <https://www.icmec.org/wp-content/uploads/2015/10/Trends-in-Online-Crime-Feb.-2011.pdf>.

1. Garner, B. A., Black, H. C. Black's law dictionary // St. Paul: «West Group», 9th ed, 2009.

Handbook on the optional protocol on the sale of children, child prostitution and child pornography [Electronic Resource] // UNICEF, Innocenti Research Centre. Режим доступа : https://www.unicef-irc.org/publications/pdf/optional\_protocol\_eng.pdf

1. Hauck, P., Peterke, S. International Law and Transnational Organised Crime. Oxford: Oxford University Press, 2016.

Kiyuna. A., Conyers, L., Cyberwarfare Sourcebook // Lulu.com, 2015.

1. Kshetri, N. The Global Cybercrime Industry / Berlin, Springe, 2010.
2. Kulesza, J. International Internet Law // Routlege, New York, 2012.
3. Lewis, J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, Washington, December 2002.
4. Murray, A. Information Technology Law: The Law and Society // 2nd ed, Oxford University Press, 2010.
5. Mwaita, P., Owor, M. Workshop report on effective cybercrime legislation in Eastern Africa [Electronic Resource] / Tanzania, 22-24 August 2013. Режим доступа : <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2349>
6. Natsui, T. Cybercrimes In Japan: Recent Cases, Legislations, Problems And Perspectives // Meiji Law Journal vol.10. 2003.
7. Ogun, M. N. Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purpose // Journal of Applied Security Research, Vol. 7, Issue 2, 2012.
8. Qijun Gu, Peng Liu, Denial of Service Attacks [Electronic Resource] // Penn State Cyber Security Lab, Режим доступа: <https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf>
9. Raja Rao, C., Guha, S. K. Principles of Medical Electronics and Biomedical Instrumentation // Universities Press (India) Ltd, 2000.
10. Reich, P.C. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization // Centre for International Studies, Dublin City University, 2008.
11. Schabas, W. A. An introduction to the International Criminal Court. 3rd edn. Cambridge: Cambridge University Press, 2007.
12. Schmitt, M. N. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. The National Academies Press, Washington D.C., 2010.
13. Schjolberg S. Computers and Penal Legislation – A Study of the Legal Politics of a new Technology / CompLex 3/86, Universitetsforlaget. Norway. 1983
14. Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva [Electronic Resource] : December 2008. Режим доступа : http://cybercrimelaw.net/documents/cybercrime\_history.pdf
15. Sofaer, A. D., Goodman, S. E. Cyber Crime and Security: The Transnational Dimension / Sofaer, A. D., Goodman, S. E., & Cuéllar, M.-F. // The Transnational Dimension of Cyber Crime and Terrorism. CA: Hoover Institution Press, Stanford University, 2001.

Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism [Electronic Resource] // Stanford Edu, 2000. Режим доступа : http://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf

1. Taliharm, A.-M., Cyberterrorism: in Theory or in Practice? // Defence Against Terrorism Review, Vol.3, No. 2, Fall 2010.
2. The Criminal Justice Resource Manual on Computer Crime / Parker, D. B. - Washington, D.C. : U.S. Dept. of Justice, National Institute of Justice, Office of Justice Programs, 1989.
3. The Princeton Principles on Universal Jurisdiction // Princeton University, New Jersey, 2001.

Wall, D.S. Policing Cybercrimes: Situating the Public Police in Networks of Security within

1. Cyberspace // Police Practice & Research: An International Journal, vol. 8(2), 2007.
2. Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age, // Polity Press, Cambridge, 2007.
3. Wilmshurst, E. International Law and the Classification of Conflicts // Oxford: Oxford University Press, 2012.

**Иные источники**

Критическая Инфраструктура [Электронный ресурс] // Panda Security Режим доступа : <http://www.pandasecurity.com/mediacenter/pandalabs/whitepaper-critical-infrastructure/>

Утечка секретных документов "угрожает безопасности США [Электронный ресурс] // Русская служба BBC.com, 26 июля 2010. Режим доступа : http://www.bbc.com/russian/international/2010/07/100721\_us\_wikileaks.shtml?print=1

Чем занимается компания ICANN? [Электронный ресурс] // ICANN. Режим доступа : <https://www.icann.org/resources/pages/what-2012-02-25-ru>

Anonymous [Electronic Resource]. Режим доступа : <http://www.anonews.co/>

Argonne researchers 'hack' Diebold e-voting system [Electronic Resource] // Computerworld.com Режим доступа : <http://www.computerworld.com/article/2511508/security0/argonne-researchers--hack--diebold-e-voting-system.html>

Chart of signatures and ratifications of Treaty 185 (Convention on Cybercrime) [Electronic Resource] // Treaty Office, Council of Europe Portal. Режим доступа : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>

1. New Zealand’s Cyber Security Strategy // 2015, Ministry for Communications
2. Organised Crime in Europe: The Threat of Cybercrime – Situation Report 2004 / Council of Europe, March 2005.
   1. Oxford Dictionary [Electronic Resource] // Режим доступа : <https://en.oxforddictionaries.com/>

Status of Ratification [Electronic Resource] // United Nations Human Rights, Office of the High Commissioner. Режим доступа : <http://indicators.ohchr.org/>

Status : United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances [Electronic Resource] // United Nations Treaty Collection. Режим доступа : https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\_no=VI-19&chapter=6&clang=\_en

Zetter K. Group Posts E-Mail Hacked From Palin Account [Electronic Resource] // Wired.com. Режим доступа : <https://www.wired.com/2008/09/group-posts-e-m>

1. Parker, D. B. The Criminal Justice Resource Manual on Computer Crime // Washington, D.C. : U.S. Dept. of Justice, National Institute of Justice, Office of Justice Programs. 1989. [↑](#footnote-ref-1)
2. R v Gold, 1988, 1 AC 1063 [↑](#footnote-ref-2)
3. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. Para 2.1. URL : <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>

   Примечание: здесь и далее – источники по состоянию на 10.05.2017 [↑](#footnote-ref-3)
4. Sofaer, A. D., Goodman, S. E. Cyber Crime and Security: The Transnational Dimension / Sofaer, A. D., Goodman, S. E., & Cuéllar, M.-F. // The Transnational Dimension of Cyber Crime and Terrorism. CA: Hoover Institution Press, Stanford University, 2001. P.7 [↑](#footnote-ref-4)
5. United Nations Manual on the prevention and control of computer-related crime / International Review of Criminal Policy, United Nations publication, Sales No. E.94.IV.5. New York. 1994. P. 4, para 21 [↑](#footnote-ref-5)
6. Ibid. P. 12, para 61. [↑](#footnote-ref-6)
7. Act to combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence [Electronic Resource] : Chapter 08:06, Cybercrime and Computer Related Crimes, Government of Botswana, 28 December 2007. URL : <http://www.bocra.org.bw/sites/default/files/documents/CHAPTER%2008-06%20CYBERCRIME%20AND%20COMPUTER%20RELATED%20CRIMES.pdf> ; Criminal Code of the Republic of Bulgaria, Chapter Nine – A [Electronic Resource] : SG No 92/2003, Government of Republic Bulgaria. URL : <http://www.vks.bg/english/vksen_p04_04.htm> ; Law No. 2008-11 on Cybercrime [Electronic Resource] : National Assembly of Republic of Senegal, 25 January 2008. - URL : <http://www.wipo.int/edocs/lexdocs/laws/en/sn/sn008en.pdf> [↑](#footnote-ref-7)
8. Computer Crimes Act 1997, Act 563 [Electronic Resource] : 30 June 1997, Parliament of Malaysia. URL : <http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20563.pdf> ; Computer Crime

   Act No. 24 of 2007 [Electronic resource] : 13 July 2007, Parliament of the Democratic Socialist Republic of Sri Lanka. URL : <http://www.slcert.gov.lk/Downloads/Acts/Computer_Crimes_Act_No_24_of_2007(E).pdf> ; Cybercrime Act, 2007 [Electronic Resource] : 30 June 2007, National Council of Republic of Sudan. URL : <https://www.unodc.org/res/cld/document/sdn/2007/cybercrime_act_2007_html/Sudan_Cybercrime_Act_2007_EN.pdf>. [↑](#footnote-ref-8)
9. The Information Technology Act No. 21 of 2000 [Electronic Resource] : 9 June 2000, Parliament of Republic of India. URL : <http://meity.gov.in/writereaddata/files/itbill2000.pdf> ; Anti-Cyber Crime Law, Royal Decree No. M/17

   8 Rabi 1 1428 [Electronic Resource] : 26 March 2007, Kingdom of Saudi Arabia. URL : <http://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf> ; Ley Especial Contra Los Delitos Informáticos [Electronic Resource] : 30 de octubre de 2001, La Asamblea Nacional De La República Bolivariana De Venezuela. URL : <http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf> ; Law on Technology Transfer No. 80/2006/QH11 [Electronic Resource] : 25 December 2001, National Assembly of the Socialist Republic of Vietnam. URL : <http://www.wipo.int/edocs/lexdocs/laws/en/vn/vn050en.pdf>. [↑](#footnote-ref-9)
10. Comprehensive Study on Cybercrime [Electronic Resource] // United Nations Office on Drugs and Crime, United Nations, New York, 2013. URL : <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>. [↑](#footnote-ref-10)
11. Crimes related to computer networks : Background paper for the workshop on crimes related to computer network // A/CONF.187/10. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000. P. 6. [↑](#footnote-ref-11)
12. Ibid. P. 8. Para 21. [↑](#footnote-ref-12)
13. Ibid. P. 18. Para 56 . [↑](#footnote-ref-13)
14. Comprehensive Study on Cybercrime [Electronic Resource] // United Nations Office on Drugs and Crime, United Nations, New York, 2013. P.xvii. URL : <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> , [↑](#footnote-ref-14)
15. Schmitt, M. Tallinn Manual on the International Law Applicable to Cyber Warfare / NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013. P. 259 [↑](#footnote-ref-15)
16. Ibid; Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series . 2001. No. 185. Art. 1(a). [↑](#footnote-ref-16)
17. Argonne researchers 'hack' Diebold e-voting system [Electronic Resource] // Computerworld.com URL : <http://www.computerworld.com/article/2511508/security0/argonne-researchers--hack--diebold-e-voting-system.html> [↑](#footnote-ref-17)
18. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 5. Art. 1(a).

    [↑](#footnote-ref-18)
19. Ibid. P.2. Para 7. [↑](#footnote-ref-19)
20. Рекомендация МСЭ-Т X.1205 (04/2008) [Электронный ресурс] // МСЭ, Сектор стандартизации электросвязи МСЭ, Серия Х: сети передачи данных, взаимосвязь открытых систем и безопасность: безопасность электросвязи. C. 2. П. 3.2.4. URL : <https://www.itu.int/rec/T-REC-X.1205-200804-I> [↑](#footnote-ref-20)
21. Марков, А. С. Цирлов, В. Л. Руководящие Указания по Кибербезопасности в Контексте ISO 27032 // Вопросы кибербезопасности. 2014. N 1(2). C.29. [↑](#footnote-ref-21)
22. Benson, M. L., Simpson S, S. White-Collar Crime: An Opportunity Perspective // New York: Routledge, 2009. P.98-10. [↑](#footnote-ref-22)
23. Schjolberg S. Computers and Penal Legislation – A Study of the Legal Politics of a new Technology / CompLex 3/86. Universitetsforlaget. Norway. 1983. 147 p. [↑](#footnote-ref-23)
24. United States v. Petersen 98 F.3d 502 (9th Cir., 1996). [↑](#footnote-ref-24)
25. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 3. Para 11(ii). [↑](#footnote-ref-25)
26. Organised Crime in Europe: The Threat of Cybercrime – Situation Report 2004 / Council of Europe, March 2005. P. 86. [↑](#footnote-ref-26)
27. United States Code //Government Printing Office, 2012 ed., Supplement 1. Title 18. Art. 1029. [↑](#footnote-ref-27)
28. Ibid. Art. 1030. [↑](#footnote-ref-28)
29. Ibid. Arts. 1466A, 2251. [↑](#footnote-ref-29)
30. Unlawful Internet Gambling Enforcement Act of 2006 // Government Printing Office, 13 October 2006, 31 U.S.C.: Money and Finance [↑](#footnote-ref-30)
31. Computer Misuse Act 1990 // 29 June 1990, United Kingdom Parliament. [↑](#footnote-ref-31)
32. Ibid. Art. 1. [↑](#footnote-ref-32)
33. Ibid. Art. 2. [↑](#footnote-ref-33)
34. Ibid. Art. 3. [↑](#footnote-ref-34)
35. Ibid. Art. 3ZA. [↑](#footnote-ref-35)
36. Cybersecurity law of the People's Republic of China // 7 November 2016, National People's Congress. Art. 32 [↑](#footnote-ref-36)
37. Ibid. Art. 22. [↑](#footnote-ref-37)
38. Electronic Communications and Transactions Act 25 of 2002 // 31 July 2002, Parliament of the Republic of South Africa. Art. 85 ; Qatar National Cyber Security Strategy // May 2014, Ministry of Information and Communications Technology. P. 23. [↑](#footnote-ref-38)
39. New Zealand’s Cyber Security Strategy // 2015, Ministry for Communications. P. 12; Cyber Security Strategy // 2009, Attorney General’s Department, Commonwealth of Australia. [↑](#footnote-ref-39)
40. Kshetri, N. The Global Cybercrime Industry / Berlin, Springer, 2010. P. 3. [↑](#footnote-ref-40)
41. Comprehensive Study on Cybercrime [Electronic Resource] // United Nations Office on Drugs and Crime, United Nations, New York, 2013. P.11-22. URL : <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> . [↑](#footnote-ref-41)
42. Garner, B. A., Black, H. C. Black's law dictionary // St. Paul: «West Group», 9th ed, 2009. [↑](#footnote-ref-42)
43. Oxford Dictionary [Electronic Resource] // URL : https://en.oxforddictionaries.com/ [↑](#footnote-ref-43)
44. Crimes related to computer networks : Background paper for the workshop on crimes related to computer network // A/CONF.187/10. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000. P. 4. [↑](#footnote-ref-44)
45. Draft Code of Crimes against the Peace and Security of Mankind with commentaries // Yearbook of the International Law Commission. 1996. Vol. II, Part Two. P. 17. Art. 1(2). [↑](#footnote-ref-45)
46. Верле, Г. Принципы международного уголовного права: учебник / пер. с англ. С.В. Саяпина. М.: ТрансЛит, 2011. С. 56. [↑](#footnote-ref-46)
47. Draft Code of Crimes against the Peace and Security of Mankind with commentaries // Yearbook of the International Law Commission. 1996. Vol. II, Part Two. Art.16. [↑](#footnote-ref-47)
48. Ibid. Art. 17. [↑](#footnote-ref-48)
49. Ibid. Art. 18 . [↑](#footnote-ref-49)
50. Ibid. Art. 19. [↑](#footnote-ref-50)
51. Ibid. Art. 20. [↑](#footnote-ref-51)
52. Bassiouni, M. C. International Criminal Law. Transnational Publishers, Inc., Ardsley, 1999. P. 32 ; Schabas, W. A. An introduction to the International Criminal Court. 3rd edn. Cambridge: Cambridge University Press, 2007. P.88. [↑](#footnote-ref-52)
53. Crawford J., Brownlie I. Brownlie's principles of public international law. 8th ed. Oxford: Oxford University Press, 2012. p. 690. [↑](#footnote-ref-53)
54. Определение агрессии // Резолюция Генеральной Ассамблеи 3314 (XXIX) от 14 декабря 1974, Официальные отчеты Генеральной Ассамблеи, двадцать девятая сессия, Приложение, № 31. Ст. 1. [↑](#footnote-ref-54)
55. Amendment to the Rome Statute of the International Criminal Court on the Crime of Aggression, articles 8bis, 15bis and 15ter, 11 June 2010 [Electronic Resource] // Resolution RC/Res.6 of 11 June 2010. Art. 8-bis. URL : <https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf> [↑](#footnote-ref-55)
56. Ibid. Art. 3. [↑](#footnote-ref-56)
57. Ibid. Art. 4. [↑](#footnote-ref-57)
58. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ) Report, 27 June 1986. Paras 188-190. [↑](#footnote-ref-58)
59. Устав ООН // 1 UNTS XVI, 26 июня 1945. Ст. 51. [↑](#footnote-ref-59)
60. Draft Articles on Responsibility of States for Internationally Wrongful Acts // Report of the International Law Commission on the Work of its 53rd sess., UNGAOR, 56th sess., sup. No. 10 (A/56/10), ch. IV.E.1. P. 128. [↑](#footnote-ref-60)
61. Schmitt, M. N. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. The National Academies Press, Washington D.C., 2010. P. 151. [↑](#footnote-ref-61)
62. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ) Report, 27 June 1986. Para 228. [↑](#footnote-ref-62)
63. Schmitt, M. N. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. The National Academies Press, Washington D.C., 2010. P.155. [↑](#footnote-ref-63)
64. Schmitt, M. Tallinn Manual on the International Law Applicable to Cyber Warfare / NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013. P. 45, 47. [↑](#footnote-ref-64)
65. Amendment to the Rome Statute of the International Criminal Court on the Crime of Aggression, articles 8bis, 15bis and 15ter, 11 June 2010 [Electronic Resource] // Resolution RC/Res.6 of 11 June 2010. Elements of Crimes. Art. 8-bis. Element 3. URL : https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf [↑](#footnote-ref-65)
66. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986. Para 115. [↑](#footnote-ref-66)
67. Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries. // Yearbook of the International Law Commission, 2001, vol. II, Part Two. P. 111-112. [↑](#footnote-ref-67)
68. Ibid. Art. 11. [↑](#footnote-ref-68)
69. Rome Statute of the International Criminal Court // A/CONF.183/9, UN General Assembly, 17 July 1998. Art. 8. [↑](#footnote-ref-69)
70. Raja Rao, C., Guha, S. K. Principles of Medical Electronics and Biomedical Instrumentation // Universities Press (India) Ltd, 2000. P. 177-201. [↑](#footnote-ref-70)
71. Международное право. Особенная часть : учеб. для студентов юрид. фак. и вузов / И.И. Лукашук;

    Рос. акад. наук, Ин-т государства и права, Академ. правовой ун-т. — Изд. 3-е, перераб. и доп. — М. :

    Волтерс Клувер, 2005. С. 430 [↑](#footnote-ref-71)
72. Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva [Electronic Resource] : December 2008. URL : http://cybercrimelaw.net/documents/cybercrime\_history.pdf [↑](#footnote-ref-72)
73. Конвенция Организации Объединенных Наций против транснациональной организованной преступности // Резолюция Генеральной Ассамблеи 25, прил. I, 55 Сессия. U.N. Doc. A/45/49, Том. I, 2001. Ст. 3(2) [↑](#footnote-ref-73)
74. Hauck, P., Peterke, S. International Law and Transnational Organised Crime. Oxford: Oxford University Press, 2016. P. 224. [↑](#footnote-ref-74)
75. Ibid. P. 336. [↑](#footnote-ref-75)
76. Choo, K.-K. R., Grabosky, P. Cyber Crime // L. Paoli, Oxford Handbook of Organized Crime. Oxford: Oxford University Press, 2013. DOI: 10.1093/oxfordhb/9780199730445.013.003. P. 485 [↑](#footnote-ref-76)
77. Ibid, P. 486. [↑](#footnote-ref-77)
78. Ibid. [↑](#footnote-ref-78)
79. Anonymous [Electronic Resource]. URL : <http://www.anonews.co/> [↑](#footnote-ref-79)
80. Financial Coalition Against Child Pornography : Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography [Electronic Resource] : 1 February 2011, Financial Coalition Against

    Child Pornography. P.2 URL : <https://www.icmec.org/wp-content/uploads/2015/10/Trends-in-Online-Crime-Feb.-2011.pdf>. [↑](#footnote-ref-80)
81. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] // Сектор развития Электросвязи, Международный Союз Электросвязи. P. 44. URL : <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf> [↑](#footnote-ref-81)
82. Mwaita, P., Owor, M. Workshop report on effective cybercrime legislation in Eastern Africa [Electronic Resource] / Tanzania, 22-24 August 2013. P. 6-12. URL : <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2349> [↑](#footnote-ref-82)
83. Boister N., Currie R.J. Routledge Handbook of Transnational Criminal Law. Routledge, 2015. P. 416 [↑](#footnote-ref-83)
84. Конвенция Организации Объединенных Наций против транснациональной организованной преступности // Резолюция Генеральной Ассамблеи 25, прил. I, 55 Сессия. U.N. Doc. A/45/49, Том. I, 2001. Ст. 29(1)(h). [↑](#footnote-ref-84)
85. Подготовительные материалы, касающиеся переговоров о разработке Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Протоколов к ней / Управление Организации Объединенных Наций по наркотикам и преступности, ООН, Нью-Йорк, 2006. С. 35. [↑](#footnote-ref-85)
86. Boister N., Currie R.J. Routledge Handbook of Transnational Criminal Law. Routledge, 2015. P. 417. [↑](#footnote-ref-86)
87. Доклад совещания Межсессионной межправительственной группы экспертов открытого состава для разработки предварительного проекта возможной всеобъемлющей международной конвенции против организованной транснациональной преступности (Варшава, 2-6 февраля 1998 года) // E/CN.15/1998/5, 18 февраля 1998, Экономический и Социальный Совет, ООН. С. 17-20. [↑](#footnote-ref-87)
88. Подготовительные материалы, касающиеся переговоров о разработке Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Протоколов к ней / Управление Организации Объединенных Наций по наркотикам и преступности, ООН, Нью-Йорк, 2006. Сноски 5, 17-19, С. 12. [↑](#footnote-ref-88)
89. Доклад совещания Межсессионной межправительственной группы экспертов открытого состава для разработки предварительного проекта возможной всеобъемлющей международной конвенции против организованной транснациональной преступности (Варшава, 2-6 февраля 1998 года) // E/CN.15/1998/5, 18 февраля 1998, Экономический и Социальный Совет, ООН. С. 8. П. 19. [↑](#footnote-ref-89)
90. Например: Международная конвенция о борьбе с финансированием терроризма // Резолюция Генеральной Ассамблеи 54/109, прил. 1, 54 Сессия, U.N.T.S. 2178. С.197-293. [↑](#footnote-ref-90)
91. The use of the Internet for terrorist purposes [Electronic Resource] // United Nations Office on Drugs And Crime, UN, New York, 2012. P. 18, para 51. URL : <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> [↑](#footnote-ref-91)
92. Международная конвенция о борьбе с финансированием терроризма // Резолюция Генеральной Ассамблеи 54/109, прил. 1, 54 Сессия, U.N.T.S. 2178. Ст. 2. [↑](#footnote-ref-92)
93. Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, STL-11-01/I // Special tribunal for Lebanon, Appeals Chamber, 16 February 2011. P.38-74. [↑](#footnote-ref-93)
94. Terrorism Act 2000 // 2000, Parliament of the United Kingdom. Section 1(2)(b). [↑](#footnote-ref-94)
95. United States Code // 2012 ed., Supplement 1. Title 18. Art. 2331(1)(c). [↑](#footnote-ref-95)
96. Baranetsky, V. What is cyberterrorism? Even experts can’t agree [Electronic Resource] // The Harvard Law Record, 5 November 2009. URL : <http://hlrecord.org/2009/11/what-is-cyberterrorism-even-experts-cant-agree/> [↑](#footnote-ref-96)
97. Lewis, J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, Washington, December 2002. P.1 [↑](#footnote-ref-97)
98. Denning, D. Testimony before the Special Oversight Panel on Terrorism // Committee on Armed Services, U.S. House of Representatives, 2000. P.1. [↑](#footnote-ref-98)
99. Wamala F. National Cybersecurity Strategy Guide 2011 [Electronic resource] / ITU, 2011. С. 25. URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [↑](#footnote-ref-99)
100. Lewis, J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, Washington, December 2002. P.3. [↑](#footnote-ref-100)
101. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства [Электронный ресурс] // ОБСЕ, Вена: Ueberreuter Print GmbH, 2013. С. 17 URL: http://www.osce.org/ru/secretariat/110472?download=true [↑](#footnote-ref-101)
102. Conway, M., Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures: Working Papers in International Studies // Centre for International Studies, Dublin City University, 2008. P. 12 [↑](#footnote-ref-102)
103. Reich, P.C. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization // Centre for International Studies, Dublin City University, 2008. P. 287 [↑](#footnote-ref-103)
104. Ogun, M. N. Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purpose // Journal of Applied Security Research, Vol. 7, Issue 2, 2012. P. 209. [↑](#footnote-ref-104)
105. Zetter K. Group Posts E-Mail Hacked From Palin Account [Electronic Resource] // Wired.com. URL : <https://www.wired.com/2008/09/group-posts-e-m> [↑](#footnote-ref-105)
106. Утечка секретных документов "угрожает безопасности США [Электронный ресурс] // Русская служба BBC.com, 26 июля 2010. URL : http://www.bbc.com/russian/international/2010/07/100721\_us\_wikileaks.shtml?print=1 [↑](#footnote-ref-106)
107. Kiyuna. A., Conyers, L., Cyberwarfare Sourcebook // Lulu.com, 2015. P. 90. [↑](#footnote-ref-107)
108. Taliharm, A.-M., Cyberterrorism: in Theory or in Practice? // Defence Against Terrorism Review, Vol.3, No. 2, Fall 2010. P. 62 [↑](#footnote-ref-108)
109. См., например: Критическая Инфраструктура [Электронный ресурс] // Panda Security URL : <http://www.pandasecurity.com/mediacenter/pandalabs/whitepaper-critical-infrastructure/> [↑](#footnote-ref-109)
110. Wilmshurst, E. International Law and the Classification of Conflicts // Oxford: Oxford University Press, 2012. P. 464. [↑](#footnote-ref-110)
111. T-CY Guidance Note #11 (Draft) : Aspects of Terrorism covered by the Budapest Convention // Cybercrime Convention Committee, Council of Europe, Strasbourg, 4 October 2016. 5 p. [↑](#footnote-ref-111)
112. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] // Сектор развития Электросвязи, Международный Союз Электросвязи. P. 39. URL : <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf> [↑](#footnote-ref-112)
113. Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ // U.N.T.S.1582, 1988. Ст. 3(1)(a)(i) [↑](#footnote-ref-113)
114. Там же. Ст. 3(1)(a)(ii). [↑](#footnote-ref-114)
115. Там же. Ст. 3(1)(a)(v). [↑](#footnote-ref-115)
116. Там же. Ст. 3(1)(b)(ii). [↑](#footnote-ref-116)
117. Единая конвенция о наркотических средствах 1961 года с поправками, внесенными в нее в соответствии с Протоколом о поправках к Единой конвенции о наркотических веществах 1961 года // U.N.T.S. 976, 1975. P. 223. [↑](#footnote-ref-117)
118. Конвенция о психотропных веществах // U.N.T.S. 1019, 1971. p. 273. [↑](#footnote-ref-118)
119. Status : United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances [Electronic Resource] // United Nations Treaty Collection. URL : https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\_no=VI-19&chapter=6&clang=\_en [↑](#footnote-ref-119)
120. Status of Ratification [Electronic Resource] // United Nations Human Rights, Office of the High Commissioner. URL : <http://indicators.ohchr.org/> [↑](#footnote-ref-120)
121. Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии // Резолюция Генеральной Ассамблеи 54/263, 25 мая 2000, U.N.T.S. 2173. Преамбула, п.6. [↑](#footnote-ref-121)
122. Consideration of Reports submitted by States Parties under the OPSC, Concluding Observations on Turkey, CRC/C/OPSC/TUR/CO/1 // United Nations Committee on the Rights of the Child, 9 June 2006. Paras. 17-19; on Viet Nam, op. cit., paras. 10-11; on Costa Rica, op. cit., paras. 14-15; on Sudan, op. cit., paras. 23-24; on France, op. cit., paras. 16-17; and on Chile, paras. 22-23. [↑](#footnote-ref-122)
123. Bowker, A. Cybercrime Handbook for Community Corrections: Managing Offender Risk in the 21st Century // Charles C Thomas Pub Ltd, 2012. P. 8 [↑](#footnote-ref-123)
124. R. v. Sharpe, 2001 SCC 2. Para 166. [↑](#footnote-ref-124)
125. R. v. Sharpe, 2001 SCC 2. Para 180. [↑](#footnote-ref-125)
126. 18 U.S.C. §§ 2252(a)(4)(B) and 2256 (1994 & Supp. IV 1998), United States v. Hilton, 167 F.3d 61 (1st Cir. 1999). p. 72 [↑](#footnote-ref-126)
127. Combating the sexual abuse and sexual exploitation of children and child pornography, Directive 2011/93/EU // OJ L 335 of 17.12.2011. Art. 2(e). [↑](#footnote-ref-127)
128. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 9(2). Cм. также R. v. Oliver and Others [2003] 2 Cr.App.R. (S) 64; Attorney General v Makamian (Aram), Appeal Decision, Criminal Appeal No 258/06, ILDC 833 (CY 2007), 19th July 2007, Cyprus; Supreme Court [Sup Ct]; Supreme Court as Court of Appeal; Criminal Division [↑](#footnote-ref-128)
129. Handbook on the optional protocol on the sale of children, child prostitution and child pornography [Electronic Resource] // UNICEF, Innocenti Research Centre. P. 20. URL : https://www.unicef-irc.org/publications/pdf/optional\_protocol\_eng.pdf [↑](#footnote-ref-129)
130. Statute of the Council of Europe // European Treaty Series, Nos 1/6/7/8/11, 5 May 1949. Art. 22. [↑](#footnote-ref-130)
131. Chart of signatures and ratifications of Treaty 185 (Convention on Cybercrime) [Electronic Resource] // Treaty Office, Council of Europe Portal. URL : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> [↑](#footnote-ref-131)
132. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 2. Para. 10. [↑](#footnote-ref-132)
133. Recommendation No. R (89) 9 of the Committee of Ministers to Member Stares on Computer-related Crime // Council of Europe, Committee of Ministers, 13 September 1989, 428th meeting of the Ministers’ Deputies. [↑](#footnote-ref-133)
134. Recommendation No. R (95) 13 // Council of Europe, Committee of Ministers, 11 September 1995, 543rd meeting of the Ministers’ Deputies. [↑](#footnote-ref-134)
135. Decision No CM/Del/Dec(97)583 // 4 February 1997, Committee of Ministers (The Committee of Experts on Crime in Cyber-space). [↑](#footnote-ref-135)
136. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 2. Para. 9. [↑](#footnote-ref-136)
137. Ibid. P.4. Para 16. [↑](#footnote-ref-137)
138. Ibid. P. 7. Para 34. [↑](#footnote-ref-138)
139. Ibid. P. 9. Para 46. [↑](#footnote-ref-139)
140. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 3. [↑](#footnote-ref-140)
141. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 10. Para. 53. [↑](#footnote-ref-141)
142. Ibid. P. 13. Para 61. [↑](#footnote-ref-142)
143. Ibid. P. 13 Para 65. [↑](#footnote-ref-143)
144. Ibid. P.12. Para 69. [↑](#footnote-ref-144)
145. Ibid. P. 11. Para 67. [↑](#footnote-ref-145)
146. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 11. [↑](#footnote-ref-146)
147. Ibid. Art. 12. [↑](#footnote-ref-147)
148. Ibid. Art. 13. [↑](#footnote-ref-148)
149. Hauck, P., Peterke, S. International Law and Transnational Organised Crime. Oxford: Oxford University Press, 2016. P. 342. [↑](#footnote-ref-149)
150. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 14(2). [↑](#footnote-ref-150)
151. Ibid. Art. 14(3). [↑](#footnote-ref-151)
152. Ibid. Art. 16(1) . [↑](#footnote-ref-152)
153. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 10. Para. 152-153. [↑](#footnote-ref-153)
154. Ibid. Para 155. [↑](#footnote-ref-154)
155. Ibid. Para 154. [↑](#footnote-ref-155)
156. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 18(1). [↑](#footnote-ref-156)
157. Halford v. UK // ECtHR, App. N 20605/92, 25 June 1997. Para 41 ; Zakharov v. Russia // ECtHR, App. N 47143/06, 4 December 2015. Paras 227-305. [↑](#footnote-ref-157)
158. Explanatory Report to the Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series. 2001. N 185. P. 10. Para. 234. [↑](#footnote-ref-158)
159. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 22(5). [↑](#footnote-ref-159)
160. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 35. [↑](#footnote-ref-160)
161. Ibid. Art. 39. [↑](#footnote-ref-161)
162. Commonwealth Cybercrime Initiative [Electronic Resouce] // The Commonwealth. URL : http://thecommonwealth.org/commonwealth-cybercrime-initiative [↑](#footnote-ref-162)
163. Report of the Transborder Group for 2013, T-CY (2013)30 // Ad-hoc Subgroup on Transborder Access and Jurisdiction, Cybercrime Convention Committee, Strasbourg, 5 November 2013. [↑](#footnote-ref-163)
164. T-CY Guidance Note #1: On the notion of “computer system”, Article 1.a Budapest Convention on Cybercrime, T-CY(2012)21// Cybercrime Convention Committee, Strasbourg, 5 December 2012. [↑](#footnote-ref-164)
165. T-CY Guidance Note #8: SPAM, T-CY(2014)20 // Cybercrime Convention Committee, Strasbourg, 3 December 2014 [↑](#footnote-ref-165)
166. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 36(3). [↑](#footnote-ref-166)
167. Chart of signatures and ratifications of Treaty 185 (Convention on Cybercrime) [Electronic Resource] // Treaty Office, Council of Europe Portal. URL : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> [↑](#footnote-ref-167)
168. eEurope 2005: An information society for all, COM (2002) 263 // Commission of The European Communities, Brussels, 2002. [↑](#footnote-ref-168)
169. Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01) // The Council of the European Union, Official Journal (Information and Notices)329 , 04/11/1996. P. 1-6 ; Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC) // The Council of the European Union, Official Journal (Legislation) 270, 7.10.1998. P. 48–55 [↑](#footnote-ref-169)
170. Council Framework Decision of 24 February 2005 on attacks against information systems (2005/222/JHA) // The Council of European Union, Official Journal (Legislation) 69, 16.3.2005. P. 67–71 [↑](#footnote-ref-170)
171. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // Official Journal (Legislation) 024 , 30/01/1998. P. 1 -8. Art. 4 ; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal (Legislation) 281, 23.11.1995. p. 31–50. Art. 17. [↑](#footnote-ref-171)
172. Council Framework Decision of 24 February 2005 on attacks against information systems (2005/222/JHA) // The Council of European Union, Official Journal (Legislation) 69, 16.3.2005. P. 67–71. Art. 2/ [↑](#footnote-ref-172)
173. Ibid. Art. 3. [↑](#footnote-ref-173)
174. Ibid. Art. 4. [↑](#footnote-ref-174)
175. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // European Treaty Series, No. 108, Strasbourg, 28 January 1981. [↑](#footnote-ref-175)
176. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // Official Journal (Legislation) 218, 14 August 2013, p. 8–14. Para 4. [↑](#footnote-ref-176)
177. Ibid. Para 27. [↑](#footnote-ref-177)
178. Ibid. P. 6. [↑](#footnote-ref-178)
179. Ibid. P. 7. [↑](#footnote-ref-179)
180. Ibid. Art. 9(4)(c). [↑](#footnote-ref-180)
181. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market // Official Journal (Legislation) 178 , 17/07/2000 P. 1-16. [↑](#footnote-ref-181)
182. Directive 2006/24/EC o The European Parliament and of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC // Official Journal (Legislation) 105/54 13 April 2006. P. 54–63. [↑](#footnote-ref-182)
183. Ireland v. European Parliament and Council of the European Union // 10 February 2009, C-301/06, ECLI:EU:C:2009:68. [↑](#footnote-ref-183)
184. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal (Legislation) 281 , 23/11/1995 P. 31-50 ; Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // Official Journal (Legislation) 024 , 30/01/1998 P.1-8. [↑](#footnote-ref-184)
185. Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceeding // Official Journal (Legislation) 328/42, 15 December 2009. P. 42-47. [↑](#footnote-ref-185)
186. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) [Электронный ресурс] : // URL : <http://www.cis.minsk.by/> [↑](#footnote-ref-186)
187. Международное право / Вольфганг Граф Витцтум [и др.] ; пер. с нем., 2-е изд. 2015. П. 36. С. 577. [↑](#footnote-ref-187)
188. Там же. [↑](#footnote-ref-188)
189. Чем занимается компания ICANN? [Электронный ресурс] // ICANN. URL : <https://www.icann.org/resources/pages/what-2012-02-25-ru> [↑](#footnote-ref-189)
190. Brownlie, I. Principles of public international law // 7th(ed), Oxford University Press, 2008. P. 303. [↑](#footnote-ref-190)
191. Nottebohm Case (Liechtenstein v. Guatemala), (Second Phase) // International Court of Justice Reports, 1955. P. 4. [↑](#footnote-ref-191)
192. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 22 ; Уголовный Кодекс Российской Федерации : «Собрание законодательства Российской Федерации» № 25 от 17 июня 1996. Cт. 11. [↑](#footnote-ref-192)
193. Zippo Mfg. Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119 [↑](#footnote-ref-193)
194. Zippo Mfg. Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119, 1124. [↑](#footnote-ref-194)
195. Kulesza, J. International Internet Law // Routlege, New York, 2012.P. 6 [↑](#footnote-ref-195)
196. Antiterrorism and Effective Death Penalty ACT // 110 Stat. 1214 [↑](#footnote-ref-196)
197. Cassese, A. International Criminal Law // 2nd ed., Oxford University Press, 2008 [↑](#footnote-ref-197)
198. Римский Статут // A/CONF.183/9, 17 июля 1998, U.N. T. S, vol. 2187, No. 38544. Ст. 12(2). [↑](#footnote-ref-198)
199. The case of the S.S. “Lotus” // Permanent Court of the International Justice, 7 September 1927, Publication of the Permanent Court of International Justice, Series A, No. 10. P. 18. [↑](#footnote-ref-199)
200. The case of the S.S. “Lotus” // Permanent Court of the International Justice, 7 September 1927, Publication of the Permanent Court of International Justice, Series A, No. 10. P. 13-15, 32. [↑](#footnote-ref-200)
201. Kulesza, J. International Internet Law // Routlege, New York, 2012.P. 15. [↑](#footnote-ref-201)
202. Ibid. P.87-97. [↑](#footnote-ref-202)
203. The Princeton Principles on Universal Jurisdiction // Princeton University, New Jersey, 2001. p. 27 [↑](#footnote-ref-203)
204. Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium) // ICJ Reports, 2002. P. 19, 31-34. [↑](#footnote-ref-204)
205. Kulesza, J. International Internet Law // Routlege, New York, 2012.P. 16. [↑](#footnote-ref-205)
206. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 22. [↑](#footnote-ref-206)
207. Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism [Electronic Resource] // Stanford Edu, 2000. Art. 5 URL : http://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf [↑](#footnote-ref-207)
208. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. P. 20. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [↑](#footnote-ref-208)
209. Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age, // Polity Press, Cambridge, 2007. P. 49-50, 52-129 [↑](#footnote-ref-209)
210. Wall, D.S. Policing Cybercrimes: Situating the Public Police in Networks of Security within

     Cyberspace // Police Practice & Research: An International Journal, vol. 8(2), 2007. P. 185-187. [↑](#footnote-ref-210)
211. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. P. 28. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [↑](#footnote-ref-211)
212. An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes, Republic Act No. 10175 // Official Gazette, 12 September 2012, Republic of the Philippines. Sec. 4. [↑](#footnote-ref-212)
213. Ansari. N., Shevtekar A.,On the new breed of Denial of Service (DOS) attacks in the Internet // Saadawi, T. N., Jordan, L., & Army War College, Cyber infrastructure protection. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011. P. 281. [↑](#footnote-ref-213)
214. Qijun Gu, Peng Liu, Denial of Service Attacks [Electronic Resource] // Penn State Cyber Security Lab, P. 5, 14. URL: <https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf> [↑](#footnote-ref-214)
215. Computer Misuse Act 1990 // 29 June 1990, United Kingdom Parliament. Art. 3. [↑](#footnote-ref-215)
216. Criminal Code // R.S.C., Parliament of Canada, 1985, c. C-46. Art. 342.2(1) [↑](#footnote-ref-216)
217. Criminal Code Act 1995, Act No. 12 // Commonwealth of Australia. Part. 10.7. Division 475. [↑](#footnote-ref-217)
218. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 2. [↑](#footnote-ref-218)
219. Protection of Official Data: A Consultation Paper // Crown Copyright, London, 2017. Para. 7. [↑](#footnote-ref-219)
220. Convention on Cybercrime / Council of Europe, Budapest, 23 November 2001 // European Treaty Series – 2001 - No. 185. Art. 4. [↑](#footnote-ref-220)
221. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. P. 24. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [↑](#footnote-ref-221)
222. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems // European Traty Series. No.189. 2003. [↑](#footnote-ref-222)
223. German Penal Code // Federal Law Gazette, 1998. Sec. 86a. [↑](#footnote-ref-223)
224. Ibid. Sec. 184 ; An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes, Republic Act No. 10175 // Official Gazette, 12 September 2012, Republic of the Philippines. Sec. 4(c)(1). [↑](#footnote-ref-224)
225. Unlawful Internet Gambling Enforcement Act // 120 Stat. 1884, 2006. Para 5367. [↑](#footnote-ref-225)
226. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. P. 40. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [↑](#footnote-ref-226)
227. An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes, Republic Act No. 10175 // Official Gazette, 12 September 2012, Republic of the Philippines. Sec. 4(a)(6). [↑](#footnote-ref-227)
228. Natsui, T. Cybercrimes In Japan: Recent Cases, Legislations, Problems And Perspectives // Meiji Law Journal vol.10. 2003. P.6 [↑](#footnote-ref-228)
229. Dutch Criminal Code [Electronic Resource] // Legislationline. Sec. 326c. Para.1. URL : http://www.legislationline.org/documents/id/4693 [↑](#footnote-ref-229)
230. Murray, A. Information Technology Law: The Law and Society // 2nd ed, Oxford University Press, 2010. P. 429. [↑](#footnote-ref-230)
231. Advisory Report on the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999 / House of Representatives, Standing Committee on Legal and Constitutional Affairs // Parliament of the Commonwealth of Australia, 2000. Para 3.8-3.10 ; Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) // The Parliament of Australia, 2004. [↑](#footnote-ref-231)
232. Understanding Cybercrime: A Guide for Developing Countries [Electronic resource] // ITU Telecommunication Development Sector, ICT Applications and Cyber Security Division Policies and Strategies Department. P. 48. URL : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [↑](#footnote-ref-232)
233. United States Code // 2012 ed., Supplement 1. Title 18. Art. 1028, 1001 ; Identity Cards Act 2006 // Parliament of the United Kingdom, 2006. Para. 25. [↑](#footnote-ref-233)